National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

CISCO Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Virtual Private Network (VPN) Platform

Report Number: CCEVS-VR-10313-2009
Dated: 13 April 2009
Version: 1.1

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 6740
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

James Brosey
Orion Security Solutions
McLean, VA

John Nilles
Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Shukrat Abbas
Manual Cintron
Tammy Compton
Lisa Vincent
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Virtual Private Network (VPN) Platform (henceforth referred to as ASA). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in March 2009. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.1.

ASA consists of hardware and software used to construct Virtual Private Networks (VPNs). ASA is a purpose-built platform that may be used, with or independent of its firewall, intrusion prevention system, and network antivirus capabilities, as a dedicated-function VPN platform.

For VPN Services, the ASA 5500 Series provides a complete remote-access VPN solution that supports numerous connectivity options, including Cisco VPN Client for IP Security (IPSec), WebVPN, and network-aware site-to-site VPN connectivity. IPSec provides confidentiality, authenticity, and integrity for IP data transmitted between trusted (private) networks over untrusted (public) links or networks. WebVPN uses a Web browser and SSL encryption to secure connections between remote users and specific, supported internal protected resource.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This Validation Report applies only to the specific version of the TOE as evaluated. 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 provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the

testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.1) have been met.

The technical information included in this report was obtained from the Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Virtual Private Network (VPN) Platform Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 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.
- 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 ASA 5505, 5510, 5520, 5540 and 5550 (Release 7.2(4)), Cisco VPN Client Release 5.0.03.0560
Protection Profile	None
ST:	Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Virtual Private Network (VPN) Platform Security Target, Version 11.0, April 2009

Item	Identifier
Evaluation Technical Report	Evaluation Technical Report For the Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550Virtual Private Network (VPN) Platform (Proprietary),Version 4.0, April 2, 2009
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3 Part 2: Evaluation Methodology, Supplement: ALC_FLR- Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc
Developer	Cisco Systems, Inc
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	James Brosey, Orion Security Solutions, McLean, VA John Nilles, Aerospace Corporation, Columbia, MD

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Overview

The TOE is a purpose-built hardware device that uses an Intel processor in all models. The ASA runs the Cisco Adaptive Security Appliance Software "image". The TOE provides a single point of defense as well as controlled and audited access to services between networks by permitting or denying the flow of information traversing the appliance.

3.2 Virtual Private Network Concept

The TOE controls the flow of IP traffic between network interfaces. The network interfaces are either "internal" or "external". If an interface is identified as external than the network to which it attaches is classed as being outside of the TOE. If an interface is identified as an internal interface than the network to which it attaches is classed as being inside (or behind) the TOE. All networks inside (or behind) are protected by the TOE against those outside the TOE. A VPN is a secure connection between a user on the outside network communicating with the TOE (a VPN device) that in turn gives the user access to the inside network. The VPN connection is considered secure because the user is authenticated and the network traffic is protected from disclosure and modification through encryption. Once a VPN session is established, the TOE will decrypt incoming packets received from the user and encrypt outgoing packets directed to the user.

IPSec VPN is a deployment proven remote-access technology. Because IPSec can transparently support any IP application, users can work remotely (from the external network) as if they were physically in the office, attached to their office LAN (internal network). IPSec VPN connections require the Cisco VPN client software. For LAN-to-LAN IPSec. two ASAs are required.

Using only a web browser and it native SSL encryption, WebVPN provides remote access without the requirement of pre-installed VPN client software. WebVPN provides the flexibility to support secure access for users, regardless of the endpoint device they are establishing the connection from. WebVPN provides access to a broad range of web resources and both web-enabled and legacy applications from almost any computer that can reach HTTPS sites. WebVPN uses SSL and its successor, Transport Layer Security (TLS) to provide a secure connection.

3.3 TOE Physical Boundary

The TOE implements two types of physical configurations:

Remote access configurations – consisting of one ASA component which establishes and controls VPN connections and allows the flow of IP traffic between external and internal network interfaces, and a VPN Client Component executing on a physically secure, properly configured windows-based platforms.

LAN-to-LAN (Also referred to as Site-to-Site) configurations – consisting of a VPN tunnel between two ASA TOE instances connecting networks in different geographic locations.

Figure 1 depicts the TOE's physical boundary for remote access configurations. The VPN Client includes only the VPN client software, not the IT platform it runs on.

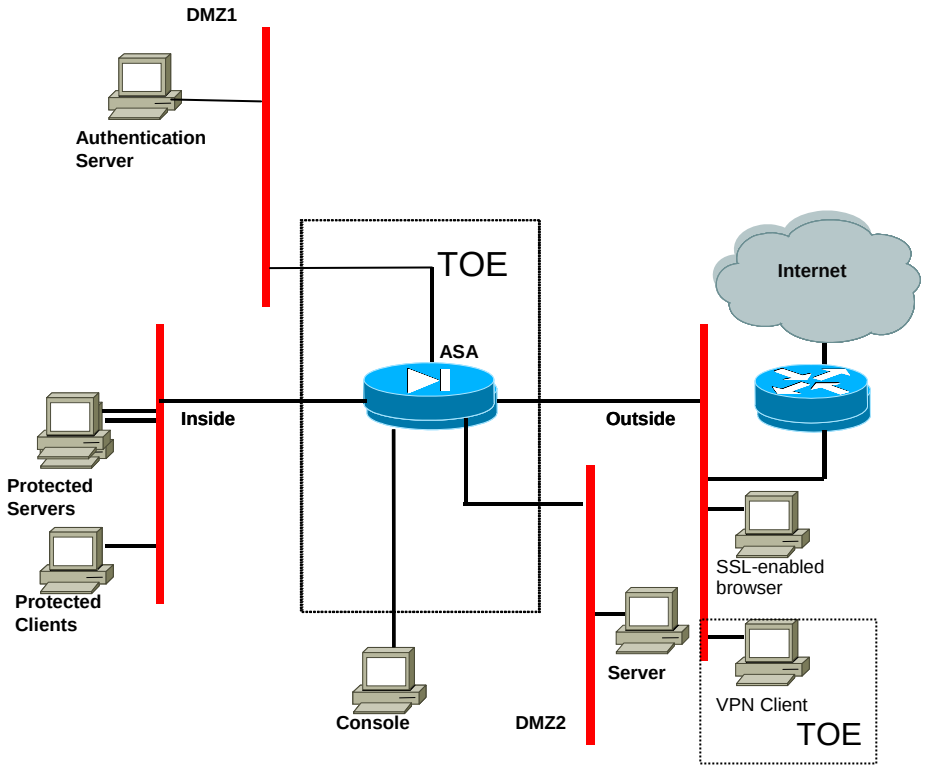

Figure 1: TOE Physical Boundary – Remote Access Configuration

The physical scope of the TOE includes the hardware and software elements identified in Table 1.

Table 1: TOE Component Identification

Hardware	ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 each with up to nine interfaces and the following processors: 5505- 500 MHz AMD GX3 5510 – 1.6 GHz Celeron 5520 – 2.0 GHz Celeron 5540 – 2.4 GHz Desktop 5550- 3.0 GHz Pentium 4
Software	Cisco Adaptive Security Appliance 'image' version 7.2(4)
	Cisco VPN Client Release 5.0.03.0560

The ASA 5500 series Adaptive Security Appliances only differ in hardware configuration and do not affect how the security functions specified in the ST are met. They are

configurable with additional modules. As well as the built-in network interfaces, the following network module is supported in this evaluation: 4-port 10/100/Gigabit Ethernet Module (part number ASA-SSM-4GE). All ASA 5500 series Adaptive Security Appliances are available with either AC or DC power. As the power supplies do not provide any security enforcing functionality the AC and DC powered models are treated identically. The software executing on all the appliances is the same version of Cisco Adaptive Security Appliance "image' version 7.2(4).

The TOE provides interconnections between two or more networks depending on the number of interface cards installed within the product. A combination of network cards can be installed in the ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550. The physical boundaries of the TOE are the physical port connections on the TOE external casing. One such port is to connect to the management console. Management of the TOE may be conducted either from a directly connected console (illustrated in Figure 1), or from a network console linked via SSH. There are no constraints on the location of the network console. In both cases the console must be physically protected. The consoles are not part of the TOE.

A separate secure management network is used (see DMZ1 in Figure 1) for the Authentication Server. The TOE environment includes a commercially available TACACS+ or RADIUS Authentication Server. Users with VPN clients and SSL-capable web browsers are located on the outside network. A VPN Client Component is contained on a physically secure and properly configured IT system and connected to the untrusted network via some form of network interface, under the control of the host operating system, e.g. LAN. When active, the VPN Client Component provides confidentiality, authenticity, and integrity for traffic transmitted over the untrusted network to the ASA. The ASA interacts with one VPN Client component: the Cisco VPN Client (IPSec Client component). The Cisco VPN Client for Windows is software that runs on a physically secure and properly configured Windows-based PC and is used to create and maintain an IPSec-based VPN connection to the ASA. The Cisco VPN Client is part of the TOE.

3.4 TOE Logical Boundary

The TOE offers both IPSec and SSL-based VPN services on a single platform. For IPSec VPN, users (on the outside) can access virtually any application as if they were actually attached to the inside network. The IPSec service requires the Cisco VPN client executing on a physically secure and properly configured windows-based PC to establish an IPSec VPN connection. The TOE will authenticate the VPN client using pre-shared keys or digital certificates (RSA). If successful authentication is achieved, a secure channel is established by using triple DES and AES ciphers to provide confidentiality and MD5 and SHA-1 algorithms for integrity and authenticity protection.

The TOE provides one connectivity option for SSL-based VPN services: WebVPN. WebVPN requires an SSL-capable web browser to establish an SSL-based VPN connection. WebVPN will only allow the web browser to access web resources and web-enabled applications behind the TOE until after the user has been authenticated. Authentication is achieved by digital certificates, username/password, or validating an

authentication cookie. The WebVPN implements the SSLv3 and TLS protocols with strengths up to 168 bit for Triple DES, and 128, 192, and 256 bit for AES. In general, the SSL protocol takes the application message (e.g., HTML) to be transmitted, fragments the data into manageable blocks, compresses the data, applies a message authentication code (MAC), encrypts, adds a header, and transmits the resulting unit as a TCP segment. Received data is decrypted, verified, decompressed, and reassembled and then delivered to the appropriate application.

An access control policy can be applied to VPN traffic, so individuals and groups of users have access to the applications, network services, and resources to which they are entitled. The TOE provides an authorized administrator the capability to define a single policy that incorporates both security and connectivity for remote users.

The TOE can be managed by authorized administrators via a physically secure local connection. The ASA appliance part of the TOE can also be managed remotely from a connected network, through SSH. The TOE supports the authentication of authorized administrators by means of user id and password, and, with support from the environment, supports the use of third party authentication servers.

The TOE provides audit generation and audit viewing capability via a configurable log file stored locally on the TOE.

The external authentication server used to provide authentication (if configured by the authorized administrator) is outside the scope of the TOE, although use made by the TOE of this server is within scope.

Non-Cisco clients such as an SSL-capable web browser used to establish a VPN session with the TOE is considered part of the TOE IT Environment.

3.5 TOE Features Excluded from Evaluation

The bulleted list below identifies functionality included in the TOE's physical boundary but not included in the TOE's logical boundary or claimed in the TOE's security functionality. The TOE features and hardware listed below are outside the scope of the defined TOE Security Functions (TSF) and are therefore not evaluated. The features listed below are non-interfering with the TSF.

- SSL VPN Client (SVC)
- Cut-through Proxies
- RIP
- SNMP
- DHCP Server
- Intrusion Prevention System capabilities
- TCP Port Forwarding
- Content filtering

- Anti-X capabilities
- CRACK authentication method
- Fail-over
- on the 5505: USB0, 1, and 2 ports
- on the 5510: USB1 and USB2 ports
- on the 5520: USB1 and USB2 ports;
- on the 5540: USB1 and USB2 ports;
- on the 5550: USB1 and USB2 ports

The following add-on modules were not evaluated and must be excluded from use in the TOE:

- AIP SSM (intrusion detection) and CSC SSM Content Security) modules

4 Security Policy

The Security Functional Policies (SFPs) implemented by ASA are based upon the basic set of security policies to support remote access: security management, audit, IPSec VPN, SSL VPN, Identification and Authentication, self protection and clock.

Note: Much of the description of the ASA security policy has been extracted and reworked from the ASA Security Target.

4.1 Security Management

ASA's security management functions provides security capabilities that guarantees all administrators are required to identify and authenticate to it before any administrative or monitoring actions can be performed. ASA only allows administration to occur from the console port or from a network console via SSH. ASA's Management Security Capability provides administrator support functionality that enables a human user to manage and configure the product.

4.2 Audit

ASA's security function supports audit record generation and review. The administrator can read audit records locally. ASA provides date and time information that is used in audit timestamps.

4.3 IPSec VPN

ASA implements the IETF IPSec protocols (RFCs 2401-2410) to provide confidentiality, authenticity, and integrity for packets flows transmitted from and received by ASA.

4.4 SSL VPN

ASA implements the SSLv3 and TLS protocol to provide SSL-based VPN connectivity.

4.5 Identification and Authentication

ASA's Identification and Authentication security function provides I&A support of all client hosts (VPN Client Components and SSL-capable web browser) requesting a VPN session along with providing I&A support to make sure all administrator are properly identified and authenticated.

4.6 Self Protection

ASA provides for non-bypassability and domain separation of functions within the its scope of control. To enable itself to be "self defending" the inbound filtering functions of the ASA are included. This allows (for example) IP packets that are not IPSec or SSL to be ignored by ASA, which is particularly important as ASA will typically operate with one interface facing a public network. The ASA controls actions carried out by a user by controlling a user's VPN session and the actions carried out during that session. By maintaining and controlling a VPN session a user has with it, ASA ensures that no security functions are bypassed and that there is a separate domain for itself to prevent tampering and interference.

4.7 Clock

ASA uses an internal clock to provide a source of date and time information used to produced a reliable time stamp for audit record generation.

5 Assumptions

The following assumptions were made during the evaluation of ASA:

- As the security functions of the TOE can be compromised by an authorized administrator, administrators are assumed to be non-hostile and trusted to perform their duties correctly.

- As the security functions of the TOE can be compromised by an attacker with physical access to the TOE, it is assumed that the TOE is located in a physically secure environment.

- As the security functions of the TOE can be compromised due to errors or omissions in the administration of the security features of the TOE, it is assumed

that administrators of the TOE have been trained to enable them to securely configure the TOE.

- As the security functions of the TOE when configured to use digital certificates can be compromised if the Certificate Authority (CA) that issued the certificates is not operated in a trusted manner, it is assumed that if the TOE is configured to use digital certificates, the issuing CA is trusted to at least the same level as the TOE.

- Pre-shared keys are assumed to be securely communicated between disparate administrators.

- The VPN Client Components will be installed on a physically protected, properly configured IT platform and operated in a secure manner.

6 Documentation

The following documentation was used as evidence for the evaluation of the ASA:

6.1 Configuration Management

1. Configuration Management, Lifecycle and Delivery Procedures for Cisco Adaptive Security Appliances 5505, 5510, 5520, 5540 and 5550, ASA VPN, Version 7.2(4), Reference ASAVPN-EAL4-CMP-v1-2, November 2008, Version 1.2

6.2 Delivery and Operation

1. Configuration Management, Lifecycle and Delivery Procedures for Cisco Adaptive Security Appliances 5505, 5510, 5520, 5540 and 5550, ASA VPN, Version 7.2(4), Reference ASAVPN-EAL4-CMP-v1-2, November 2008, Version 1.2
2. Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Common Criteria EAL4+ Administrator Guide For Virtual Private Networks (VPN)s, Version 8.0, November 12, 2008

6.3 Design Documentation

1. Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540, 5540 and 5550 Virtual Private Network (VPN) Platform Functional Specification, Version 6.0, October 29, 2008
2. Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540, 5540 and 5550 Virtual Private Network (VPN) Platform High Level Design, Version 4.0, February 19, 2008
3. Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540, 5540 and 5550 Virtual Private Network (VPN) Platform Low Level Design, Version 7.0, January 15, 2009

4. Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540, 5540 and 5550 Virtual Private Network (VPN) Platform TOE Security Policy Model, Revision 4.0, October 29, 2008
5. Implementation subset

6.4 Guidance Documentation

1. Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Common Criteria EAL4+ Administrator Guide For Virtual Private Networks (VPN)s, Version 8.0, November 12, 2008
2. Cisco Security Appliance Command Line Configuration Guide For the Cisco ASA 5500 Series and Cisco PIX 500 Series Software Version 7.2(2) [Text Part Number OL-10088-02]
3. Cisco Security Appliance Logging Configuration and System Log Messages For the Cisco PIX 500 Series and Cisco ASA Series Security Appliance Software Version 7.2 [Text Part Number OL-10099-01]
4. Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide, Version 7.2 For the Cisco ASA 5510, ASA 5520, and ASA 5540 [Text Part Number: 78-17644-01]
5. Cisco ASA 5505 Getting Started Guide, Version 7.2 [Text Part Number: 78-17612-02]
6. Release Notes for Cisco SSL VPN Client Release 1.1.0 [Text Part Number OL-7819-03].
7. VPN Client User Guide for Windows [Text Part Number OL-5489-01]
8. Cisco ASA 5500 Series Hardware Installation Guide [Text Part Number OL-10089-0178-16409-03]
9. Cisco ASA 5550 Getting Started Guide, Version 7.2 [Text Part Number: 78-17644-01
10. Cisco Security Appliance Command Reference Guide Version 7.2 [Text Part Number OL-10086-0102]
11. Using the Cisco ASA 5500 Series Appliance for VPN Connectivity (Cisco White Paper)
12. Migrating to ASA for VPN 3000 Concentrator Series Administrators [Text Part Number OL-6940-01]
13. Cisco ASA 5500 Release Notes 7.2(24) [Text Part Number 10103-0203]

6.5 Life Cycle

1. Development Security for Cisco Adaptive Security Appliances, Reference ASA_EAL4-DVS-v1-2.doc, November 2008, Version: 1.2, EDCS-684382

6.6 Testing

1. Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Virtual Private Network (VPN) Platform Test Coverage and Depth Analysis, Version 2.2, November 20, 2008
2. Common Criteria Detailed Test Plan Results: EDCS-602486, Rev 2

6.7 Vulnerability Assessment

1. Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540, 5540 and 5550 Virtual Private Network (VPN) Platform Misuse Analysis, Version 3.0, November 12, 2008
2. SOF Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540, and 5550, Virtual Private Network (VPN) Platform, Strength of Function, Version 3.0, November 12, 2008
3. Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540, and 5550 series, Appliance with Software Load 7.2(4) Vulnerability Analysis, Version 5.0, January 12, 2009

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Cisco ASA, Version 3.0, April 2, 2009.

7.1 Developer Testing

At EAL4, testing must demonstrate correspondence between the tests and the functional specification and high level design. The vendor testing was extensive and covered all of the security functions identified in the ST and interfaces in the design. These security functions include:

- Security Management
- Audit
- Identification and Authentication
- IPSec VPN
- SSL VPN
- Self Protection
- Clock

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the Evaluated Configuration Guide, reran a sample of the developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

The evaluation team ran its tests on the 5510 and 5520 platforms. All models of the TOE execute the same binary image and are compiled from identical source code. Additionally,

the TOE hardware that is relied upon to implement TOE security policy (e.g. system clock) is the same across all models. Since the code and hence security functionality is the same among the platforms, the evaluation team only ran tests on two platforms.

Cisco used the same argument and produced results only for the 5510 platform. The hardware and software components are summarized in the subsequent sections.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Cisco ASA 5505, 5510, 5520, 5540 and 5550 (Release 7.2(4)), Cisco VPN Client Release 5.0.03.0560.

To use the product in the evaluated configuration, the product must be configured as specified in the **Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Common Criteria EAL4+ Administrator Guide For Virtual Private Networks (VPN)s, Version 8.0, November 12, 2008** document.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL4 augmented with ALC_FLR.1 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.3 [5], [6]. The evaluation determined the Cisco ASA TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.1 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 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 policies and assumptions, a statement of security requirements claimed to be met by the ASA product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 4 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 the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from Cisco.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 4 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 the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer. The evaluation team verified the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 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, a high-level design document, a low-level design document, and a security policy model. 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.

Additionally, the evaluation team ensured that the security policy model document clearly describes the security policy rules that were found to be consistent with the design documentation.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was

conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE.

In addition to the EAL 4 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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

The evaluation team applied each EAL 4 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 performed a sample of the 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.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was

conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 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 strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.9 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 vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

- The TOE must not use add-on modules that were not evaluated with the TOE. These modules include the AIP SSM (intrusion detection) and CSC SSM Content Security) modules.
- The TOE does not have password lockout features. Use of strong password is highly recommended.
-

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Virtual Private Network (VPN) Platform Security Target, Version 11.0, April 2009.*

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.3, August 2005.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.3, August 2005.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.3, August 2005.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

[5] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 2.3 August 2005.

[6] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[7] Science Applications International Corporation. *Evaluation Technical Report for the [9] Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Virtual Private Network (VPN) Platform Part 2 (Proprietary)*, Version 4.0, April 2, 2009.

[8] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco ASA, ETR Part 2 Supplement (SAIC and Cisco Proprietary)*, Version 3.0, April 2, 2009.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Virtual Private Network (VPN) Platform Security Target, Version 11.0, April, 2009