National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Cisco Systems, Inc, 170 West Tasman Dr., San Jose, CA 95134

Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform

Report Number: CCEVS-VR-10381-2011
Dated: 11 July 2011
Version: 0.2

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 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Jandria Alexander
Aerospace Corporation
Columbia, MD

Olin Sibert
Orion Security Solutions, Inc.
McLean, VA

Common Criteria Testing Laboratory

Tammy Compton
Gary Grainger
Katie Sykes
Quang Trinh
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) Firewall and Virtual Private Network (VPN) Platform solution provided by Cisco Systems, Inc. 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 June 2011. 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.2.

The TOE is a purpose-built security platform that combines application-aware firewall and VPN services for small and medium-sized business (SMB) and enterprise application For firewall services, the ASA 5500 Series provides application-aware stateful packet filtering firewalls. The application-inspection capabilities automate the network to treat traffic according to detailed policies based not only on port, state, and addressing information, but also on application information buried deep within the packet header. 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), Cisco Clientless SSL VPN, network-aware site-to-site VPN connectivity, and Cisco AnyConnect VPN client. IPSec provides confidentiality, authenticity, and integrity for IP data transmitted between trusted (private) networks over untrusted (public) links or networks. For management purposes, the ASDM is included. ASDM allows the ASA to be managed from a graphical user interface.

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 3.1, Rev 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 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.2) have been met.

The technical information included in this report was obtained from the Cisco Adaptive Security Appliances (ASA) Firewall and 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 Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platforms, Cisco AnyConnect, Cisco VPN Client, Cisco SSL VPN (clientless), Cisco Adaptive Security Device Manager (ASDM).
TOE Hardware Models	Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580-20, and 5580-40
TOE Software Version	Cisco ASA Release 8.3.2, Cisco AnyConnect Release 2.5, Cisco VPN Client

Item	Identifier
	Release 5.0, Cisco Adaptive Security Device Manager (ASDM) 6.3.2
Protection Profile	U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments, Version 1.1, July 25, 2007
ST:	Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform Security Target, Version .18, June 2011
Evaluation Technical Report	Evaluation Technical Report For the Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform (Proprietary), Version 2.0, June 13, 2011
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3
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	Jandria, Aerospace Corporation, McLean, VA
	Olin Sibert, Orion Security Solutions, Inc., McLean, VA

3 Architectural Information

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

3.1 TOE Introduction

The TOE consists of hardware and software used to construct Virtual Private Networks (VPNs) and Firewall solutions.

For firewall services, the ASA 5500 Series provides application-aware stateful packet filtering firewalls. A stateful packet filtering firewall controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the authorized administrator for firewalls. This header information includes source and destination host (IP) addresses, source and destination port numbers, and the transport service application protocol (TSAP) held within the data field of the IP packet. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. The stateful firewall remembers the state of the connection from information gleaned from prior packets flowing on the connection and uses it to regulate current packets. The packet will be denied if the security policy is violated.

In addition to IP header information, the TOE mediates information flows on the basis of other information, such as the direction (incoming or outgoing) of the packet on any given firewall network interface. For connection-oriented transport services, the firewall either

permits connections and subsequent packets for the connection or denies the connection and subsequent packets associated with the connection.

The application-inspection capabilities automate the network to treat traffic according to detailed policies based not only on port, state, and addressing information, but also on application information buried deep within the packet header. By comparing this deep-packet inspection information with corporate policies, the firewall will allow or block certain traffic. For example, it will automatically drop application traffic attempting to gain entry to the network through an open port-even if it appears to be legitimate at the user and connection levels-if a business's corporate policy prohibits that application type from being on the network.

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), Cisco Clientless SSL VPN, network-aware site-to-site VPN connectivity, and Cisco AnyConnect VPN client. IPSec provides confidentiality, authenticity, and integrity for IP data transmitted between trusted (private) networks over untrusted (public) links or networks. SSL VPN uses a Web browser and SSL encryption to secure connections between remote users and specific, supported internal protected resources. AnyConnect uses the Datagram Transport Layer Security (DTLS) and Secure Socket Layer (SSL) protocols to provide remote users with secure VPN connections to the ASA. Note: these VPN configurations are only supported in Routed Single Context Mode.

For management purposes, the ASDM is included. ASDM allows the ASA to be managed from a graphical user interface. Its features include:

- Rapid Configuration: in-line and drag-and-drop policy editing, auto complete, configuration wizards, appliance software upgrades, and online help;
- Powerful Diagnostics: Packet Tracer, log-policy correlation, packet capture, regular expression tester, and embedded log reference;
- Real-Time Monitoring: device, firewall, content security, real-time graphing; and tabulated metrics;
- Management Flexibility: A lightweight and secure design enables remote management of multiple security appliances.

3.2 Physical Scope of the TOE

This section provides an overview of the Cisco ASA Firewall and VPN Platforms Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE consists of a number of components including:

- One or more 5500 Appliances: The appliance is a single-use device with a hardened version of the Linux Kernel 2.6 (32 bit for everything but the 5580s and 64 bit for the 5580s) running ASA Release 8.3.2. Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540, ASA-5550, ASA-5580-20, and 5580-40 each with the following processor and interface configurations:

- 5505 – 500 MHz AMD GX3 – Eight 10/100 copper Ethernet ports;
- 5510 – 1.6 GHz Celeron – Five 10/100 copper Ethernet ports (two can be 10/100/1000 copper Ethernet ports), one out-of-band management port;
- 5520 – 2.0 GHz Celeron – Four 10/100/1000 copper Ethernet ports, one out-of-band management port;
- 5540 – 2.0 GHz Pentium 4 – Four 10/100/1000 copper Ethernet ports, one out-of-band management port;
- 5550 – 3.0 GHz Pentium 4 – Eight Gigabit Ethernet ports, four small form factor-pluggable (SFP) fiber ports, one Fast Ethernet port;
- 5580-20 – Four 2.6GHz AMD Opteron – Two RJ-45 management ports, two Gigabit Ethernet management ports, with space for 6 interface expansion cards:

Up to twelve 10Gigabit Ethernet (10GE) ports (two per ASA5580-2X10GE-SR card)

Up to twenty-four Gigabit Ethernet ports (four per ASA5580-4GE-FI card)

Up to twenty-four 10/100/1000 Ethernet ports (four per ASA5580-4GE-CU card)

- 5580-40 – Four 2.6GHz AMD Opteron – Two RJ-45 management ports, two Gigabit Ethernet management ports, with space for 6 interface expansion cards:

Up to twelve 10Gigabit Ethernet (10GE) ports (two per ASA5580-2X10GE-SR card)

Up to twenty-four Gigabit Ethernet ports (four per ASA5580-4GE-FI card)

Up to twenty-four 10/100/1000 Ethernet ports (four per ASA5580-4GE-CU card)

- VPN clients: The following VPN clients are included with the TOE.
  - Cisco AnyConnect Release 2.5 (including Cisco SSL VPN Clientless software)
  - Cisco VPN Client Release 5.0
- ASDM software: The ASDM 6.3.2 software is installed on the ASA server. Only the Cisco ASDM Launcher is installed locally on the management platform. The ASDM software can also be launched by connecting to the https port on the ASA

The TOE is a hardware and software solution that makes up the Cisco ASA Firewall and VPN Platforms solution. The TOE is comprised of the following:

Table 1 Physical Scope of the TOE

TOE Configuration	Hardware Configurations	Software Version
ASA 5505 	The Cisco ASA 5505 features a flexible 8-port 10/100 Fast Ethernet switch, whose ports can be dynamically grouped to create up to three separate VLANs for home, business, and Internet traffic for	ASA release 8.3.2, including a Linux Kernel 2.6

	improved network segmentation and security.	
ASA 5510 	The Cisco ASA 5510 Adaptive Security Appliance provides high-performance firewall and VPN services and five integrated 10/100 Fast Ethernet interfaces (2 can be 10/100/1000) and support for up to 100 VLANs.	ASA release 8.3.2, including a Linux Kernel 2.6
ASA 5520 	The Cisco ASA 5520 Adaptive Security Appliance provides high-performance firewall and VPN services and four Gigabit Ethernet interfaces and support for up to 150 VLANs.	ASA release 8.3.2, including a Linux Kernel 2.6
ASA 5540 	The Cisco ASA 5540 Adaptive Security Appliance provides high-performance firewall and VPN services and four Gigabit Ethernet interfaces and support for up to 200 VLANs.	ASA release 8.3.2, including a Linux Kernel 2.6
ASA 5550 	The Cisco ASA 5540 Adaptive Security Appliance provides high-performance firewall and VPN services via eight Gigabit Ethernet interfaces, four Small Form-Factor Pluggable (SFP) fiber interfaces, and support for up to 250 VLANs.	ASA release 8.3.2, including a Linux Kernel 2.6
ASA 5580-20 **ASA 5580-40** 	The Cisco ASA 5580 Adaptive Security Appliances provide six interface expansion card slots with support for up to 24 Gigabit Ethernet interfaces or up to 12 10Gigabit Ethernet interfaces or up to twenty-four 10/100/1000 Ethernet ports, and support for up to 250 VLANs.	ASA release 8.3.2, including a Linux Kernel 2.6
Cisco AnyConnect (including Cisco SSL VPN Clientless software)	Not applicable	Release 2.5
Cisco VPN Client	Not applicable	5.0
ASDM 6.3.2	Not applicable	Release 6.3.2

4 Security Policy

This section summaries the security functionality of the TOE:

1. VPN and/or Firewall Information Flow Control
2. Audit
3. Identification & Authentication
4. Management
5. Cryptography

4.1.1 VPN and/or Firewall Information Flow Control

The Information Control functionality of the TOE allows authorized administrators to set up rules between interfaces of the TOE. These rules control whether a packet is transferred from one interface to another and/or transferred encrypted based upon:

1. User identities (source and/or destination)
2. Presumed address of source subject
3. Presumed address of destination subject
4. Service used
5. Transport layer protocol
6. Security-relevant service command
7. Network interface on which the connection request occurs and is to depart

Packets will be dropped unless a specific rule or policy in an access control list (ACL) has been set up to allow the packet to pass. The order of Access Control Entries (ACEs) in an ACL is important. When the TOE decides whether to forward or drop a packet, the TOE tests the packet against the ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked such that if the ACE at the beginning of the ACL explicitly permits all traffic, no further ACEs are checked. Interface ACLs are applied first before IPSec negotiations occur in the evaluated configuration.

In providing the Information Flow Control functionality, the TOE has the ability to translate network addresses contain within a packet, called Network Address Translation. Depending upon the TOE configuration the address can be translated into a permanently defined static address, an address selected from a range or into a single address with a unique port number (Port Address Translation). Also Network Address Translation can be disabled, so that addresses are not changed when passing through the TOE.

The TOE has the ability to reject requests in which the subject specifies the route in which information flows en route to the receiving subject. Through use of protocol filtering proxies, the TOE can also reject Telnet or FTP command requests that do not conform to generally accepted, published protocol definitions.

4.1.1.1 IPSec VPN

The IPSec VPN Function includes IPSec and Internet Security Association and Key Management Protocol (ISAKMP) functionality to support VPNs. A secure connection between two IPSec peers is called a tunnel. The TOE implements ISAKMP and IPSec tunneling standards to build and manage VPN tunnels. ISAKMP and IPSec accomplish the following:

- Negotiate tunnel parameters
- Establish tunnels
- Authenticate users
- Encrypt and decrypt data
- Manage data transfer across the tunnel.

The TOE implements IPSec in two types of configurations:

- LAN-to-LAN configurations are between two IPSec security gateways, such as security appliance units or other protocol-compliant VPN devices. A LAN-to-LAN VPN connects networks in different geographic locations.
- Remote access configurations provide secure remote access for Cisco VPN clients, such as mobile users. A remote access VPN lets remote users securely access centralized network resources. The Cisco VPN client complies with the IPSec protocol and is specifically designed to work with the TOE.

In IPSec LAN-to-LAN connections, the TOE can function as initiator or responder. In IPSec remote access connections, the ASA functions only as responder. Initiators propose Security Associations (SAs); responders accept, reject, or make counter-proposals—all in accordance with configured SA parameters. To establish a connection, both entities must agree on the SAs.

The TOE IPSec implementation contains a number of functional components that comprise the IPSec VPN function. In IPSec terminology, a peer is a remote-access client or another secure gateway.

4.1.1.2 SSL VPN

SSL VPN connectivity is provided through a clientless solution and a client solution – AnyConnect. The clientless SSL VPN, which is actually branded as SSL VPN, uses the SSL (v3.1) protocol and its successor, Transport Layer Security (TLS) v1.0 to provide a secure connection between remote users and specific, supported internal resources as configured by the administrator. The TOE recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users. Establishing an SSL VPN session requires the following:

- Use of HTTPS to access the TOE. In a Web browser, remote users enter the TOE IP address in the format https://address where address is the IP address or DNS hostname of the TOE interface.
- Administrator enabling clientless SSL VPN sessions on the TOE interface that remote users connect to with the 'svc enable' command.

SSL uses digital certificates for device authentication. The TOE creates a self-signed SSL server certificate when it boots, or the administrator can install in the TOE an SSL certificate that has been issued by a defined trust point (i.e., Certificate Authority).

The user is prompted to enter a username and password. If configured, the user can be authenticated using a digital certificate. A remote RADIUS server or internal authentication server can be used to authenticate remote users. Once the user successfully authenticates to the TOE, the user continues the connection using a clientless SSL VPN connection. The clientless connection provides easy access to a broad range of web resources and web-enabled applications from almost any computer on the Internet. These include secure access to the following resources:

- Internal web sites
- Web-enabled applications
- NT/Active Directory file shares
- Email proxies, including POP3S, IMAP4S, and SMTPS

The AnyConnect client provides remote end users running Microsoft Windows Vista, Windows 7, Windows XP or Windows 2000, Linux, or Macintosh OS X, with a Cisco SSL VPN client, and supports applications and functions that are unavailable to a clientless, browser-based SSL VPN connection. The same client version is used for all of the various OS platforms. In addition, the AnyConnect client supports connecting to IPv6 resources over an IPv4 network tunnel. AnyConnect utilizes the SSL v3.1 and DTLS v1.0 protocol. DTLS is a standards-based SSL protocol that provides a low-latency data path using UDP, and it is specified in RFC 4347. DTLS allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. If DTLS is not enabled, SSL VPN connections connect with an SSL VPN tunnel only.

The client is configured by the authorized administrator on the ASA and can be automatically downloaded to remote users when they log in, or it can be manually installed as an application on PCs by a network administrator. After downloading, it can automatically uninstall itself after the connection terminates, or it can remain on the remote PC for future SSL VPN connections.

Authentication of AnyConnect users can be done via user ID and reusable password, or via digital certificates.

4.1.1.3 Single or Multiple Contexts

A security context is a collection of processes that exist to model the logical virtual firewall into the constraints of the hardware. Each security context (virtual device) is treated as a separate independent device with its own security policy, interfaces, administrators, and configuration file.

When the firewall is operating in single routed mode one instance of a security context is present and executing. When the firewall is configured in multiple-context mode multiple security contexts are executing simultaneously. Each context in multiple-context mode is made up of the same processes used in single routed mode, but a process establishes the "context" for a request and then sets its operating variables to use the control/data memory owned by the context. There is no difference between the processes that are running for a single instance of a context in single, routed mode or multiple-context mode. Multiple contexts are similar to having multiple stand-alone devices.

The ASA 5505 does not support multiple contexts. Its only separation support is creation of up to 20 VLANs on its eight switch ports. The other platforms also support VLANs (up to the amounts indicated in *Table 1*).

4.1.1.4 Routed or Transparent Mode

The security appliance can run in these two firewall modes:

- Routed mode
- Transparent mode

In routed mode, the security appliance is considered to be a router hop in the network. It can perform NAT between connected networks, and can use OSPF or passive RIP (in single context mode). Routed mode supports many interfaces. Each interface is on a different subnet. Interfaces can be shared between contexts. Note that IPv6 is only supported in Routed mode.

In transparent mode, the security appliance acts like a "bump in the wire," or a "stealth firewall," and is not a router hop. The security appliance connects the same network on its inside and outside interfaces. No dynamic routing protocols or NAT are used. However, like routed mode, transparent mode also requires access lists to allow any traffic through the security appliance, except for ARP packets, which are allowed automatically. Transparent mode can allow certain types of traffic in an access list that is blocked by routed mode, including unsupported routing protocols. Transparent mode can also optionally use EtherType access lists to allow non-IP traffic. Transparent mode only supports two interfaces, an inside interface and an outside interface, in addition to a dedicated management interface, depending on the platform (all but the 5505).

NOTE: The TOE must run in Routed Single Context mode only when configured to perform VPN transmissions.

4.1.2 Audit

The TOE's Audit security function supports audit record generation and review. The TOE provides date and time information that is used in audit timestamps. The events generated by the TOE include all commands executed by the authorized administrator, in addition to cryptographic operations, traffic decisions, indication of the logging starting and stopping and other system events.

The local buffer on the ASA stores the audit records, and its size is configurable by the authorized administrator. The same protection is given to these stored events that is given to all system files on the ASA. Access to them is restricted only to the authorized administrator, who has no access to edit them, only to copy or delete (clear) them.

The audit records can be viewed either locally or remotely (via SSH v2) on the ASA CLI or through a Real-Time Log Viewer in ASDM (secured via HTTPS tunnel). The Real-Time Log Viewer in ASDM allows for filtering of events or searches by keyword and for sorting of events by the header fields in the event viewer. This allows an authorized administrator to quickly locate the information that they are looking for and quickly detect issues. This log viewer needs to be open and active during TOE operation in order to display the records as they are received.

When the buffer on the ASA reaches its capacity, the administrator will be notified that this has occurred via an alert log entry, and in order to minimize the number of events lost, new sessions through the ASA will be temporarily stopped. This will give the administrator the time to offload the audit events to another server. This can be done directly from the Real-Time Log Viewer on ASDM, where functionality is given to save the events to a local file on the host machine for backup.

4.1.3 Identification and Authentication

Authentication performed by the TOE makes use of a reusable password mechanism for access to the TOE by authorized administrators as well as by human users establishing VPN connections. The TOE by default is configured to perform local authentication and stores user names and passwords in an internal user authentication database which is only accessible by the administrator via privileged commands at the CLI or screens in ASDM. The TOE can be configured to use an external authentication server for single-use authentication such that the TOE is responsible for correctly invoking the external authentication mechanism, and for taking the correct actions based on the external server's authentication decisions.

A lockout mechanism is enforced after an administrator-specified number of failed attempts. This functionality is enforced for all locally authenticated users. The lockout results in the user being unable to authenticate until an authorized administrator unlocks the account.

VPN users are authenticated through their client (or through SSL session if clientless) to the TOE via a reusable.

4.1.4 Management

The Management functionality permits an authorized administrator from a physically secure local connection, an SSHv2 encrypted connection (the encryption is subject to FIPS PUB 140-2 security functional requirements) or an HTTPS-tunneled ASDM connection from an internal trusted host or a remote connected network to perform the following actions:

- Enable or disable the operation of the TOE.
- Enable or disable the multiple use authentication functions.
- Enable, disable, determine and modify the behavior of the audit trail management.
- Enable, disable, determine and modify the behavior of the functionality to backup and restore TSF data, information flow rules, and audit trail data.
- Enable, disable, determine and modify the behavior of communication of authorized external IT entities with the TOE.
- Delete and create attributes/ rules for VPN and information flow.
- Delete attributes from a rule, modify attributes in a rule, add attributes to a rule.
- Query, modify, delete, and assign the user attributes.
- Set the time and date used to form the timestamps.
- Specify the limits for the number of authentication failures.

All of these management functions are restricted to the authorized administrator of the TOE. The authorized administrator is defined as having the full set of privileges on the ASA, which is indicated by a level 15 privilege on a scale from 0 to 15.

All local user credentials on the ASA are stored in a central database. The users are differentiated as ASA administrators, VPN users, or cut-through proxy users through a service-type attribute and by privilege level. Only ASA administrators have any local privileges on the ASA.

Note that the VPN user role is not an administrative role, and its only purpose is to establish VPN connections to or through the TOE. It has no other privileges with respect to the TOE

4.1.5 Cryptography

The TOE relies on FIPS PUB 140-2 validation for testing of cryptographic functions. The FIPS certificate is 1436 for ASA and the clients are FIPS compliant as determined by testing by SAIC.

The Cisco VPN Client uses cryptography at two abstraction levels:

1. User space: Here cryptography is used for IKE. Once the IKE exchange is completed the keys are plumbed down to the kernel space. For supporting IKE, the

module utilizes AES, Triple-DES, HMAC-SHA-1, SHA-1, RSA (digital signatures), RSA (encrypt/decrypt), and Diffie-Hellman. These algorithms are provided by RSA Crypto-C Micro Edition dynamic library.

2. Kernel space: At this level, cryptography is used for bulk IPSec encryption/decryption and MACing. To support this, the module uses AES, Triple-DES, SHA-1 and HMAC-SHA-1 algorithms. These algorithms are provided by RSA BSAFE Crypto-Kernel library.

The Cisco AnyConnect client uses cryptography at two junctures:

1. Session setup: Here cryptography is used as part of the protocol used to set-up HTTPS sessions using TLS.
2. Data protection: Once the session set-up is complete, cryptography is used to protect data that traverses over the TLS and DTLS tunnels.

Unlike session set-up, all crypto for data protection is offloaded to the openSSL library on Windows, Linux as well as MAC OS platforms. To ensure that openSSL utilizes only FIPS approved crypto algorithms, the client has a policy file (called AnyConnectLocalPolicy) where FIPS mode can be set.

The ASA uses cryptography in the following forms:

1. Identity certificates for the ASA itself, and also for use in IPSEC, TLS, and SSH negotiations. This is provided by RSA keys.
2. Key agreement for IKE, TLS, and SSH sessions. This is provided by Diffie-Hellman.
3. For TLS traffic keys, SSH session keys, IPSec authentication keys, IPSec traffic keys, IKE authentication keys, IKE encryption keys, and key wrap for communication with an remote authentication server. These are provided in the form of AES or Triple-DES keys (with the exception of communications with an authentication server which are only in the form of AES keys).

5 Assumptions

The following assumptions were made during the evaluation of Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform:

- The TOE is physically secure.
- The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
- There are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
- The TOE does not host public data.
- Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- Information can not flow among the internal and external networks unless it passes through the TOE.

- Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
- Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.
- Authorized administrators may access the TOE remotely from the internal and external networks.

6 Documentation

The following documentation was used as evidence for the evaluation of the Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform:

6.1 Design Documentation

1. Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) 5500 Series Platforms Security Architecture Specification, Cisco, version 0.4, April 4, 2011
2. Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) 5500 Series Platforms Functional Specification, Version 0.3, March 15, 2011
3. Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) 5500 Series Platforms TOE Design Specification, Version 0.4, April 5, 2011
4. Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) 5500 Series Platforms Annex A Cisco AnyConnect Configuration Parameters, January 27, 2011
5. Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) 5500 Series Platforms Annex C Client Authentication/ Connection Error Codes, January 27, 2011
6. Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) 5500 Series Platforms Annex D WebVPN Authentication Parameters and Fields, January 27, 2011
7. Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) 5500 Series Platforms Annex E Command Interface Commands, March 15, 2011
8. Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) 5500 Series Platforms Functional Specification Annex F RFC Security Parameter Relevancy, January 27, 2011
9. Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) 5500 Series Platforms Annex G Key Destruction, January 27, 2011
10. Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) 5500 Series Platforms Annex H References for ASA VPN Platform Evidence, April 4, 2011

6.2 Guidance Documentation

1. Cisco Adaptive Security Appliance (ASA) Firewall & Virtual Private Network (VPN) Platform Preparative Procedures & Operational User Guide, Cisco, Version 0.9, June 2011
2. Release Notes for the Cisco ASA 5500 Series, 8.3(2)
3. Cisco ASA 5505 Adaptive Security Appliance Quick Start Guide, 8.3
4. Cisco ASA 5500 Series Getting Started Guide, 8.3
5. Cisco ASA 5580 Getting Started Guide, 8.3
6. ASA 5500 Migration Guide for Version 8.3
7. Cisco ASA 5500 Series Adaptive Security Appliance: Install and Upgrade Guides
8. Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series Adaptive Security Appliance
9. Cisco ASA 5500 Series Configuration Guide using the CLI, 8.3
10. Cisco ASA 5500 Series Command Reference, 8.3 [ASA 5500 Series Adaptive Security Appliances]
11. Cisco ASA 5500 Series System Log Messages, Version 8.3
12. FIPS 140-2 Non-Proprietary Security Policy for the Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580-20, and 5580-40 Security Appliances
13. Cisco ASA 5500 Series Configuration Guide using ASDM, version 6.3

6.3 Life Cycle

1. Development Security for Cisco Adaptive Security Appliances, June 2010, Version 1
2. Configuration Management, Lifecycle and Delivery Procedures for Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580-20, and 5580-40, plus the following modules AIP-SSC-5, AIP-SSM-10, AIP-SSM-20, AIP-SSM-40, and 4GE-SSM, June 2010, Version 2

6.4 Testing

1. ASA Common Criteria Test Coverage and Depth.xlsx dated 18 April 2011
2. Project ASA 8.3 Common Criteria Detailed Test Plan, which is presented in separate documents:
    a. ASA 8.3 Common Criteria Test Mappings and Introduction, Cisco, file: ASA 83 ATE Mapping and Intro.docx dated 18 April 2011
    b. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 3.1.9, 3.1.10, 3.1.11, 3.1.12, 3.1.13, 3.1.14, Cisco, file: 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.6, 3.1.8, 3.1.9, 3.1.10, 3.1.11, 3.1.12, 3.1.13, 3.1.14.docx dated 4 April 2011
    c. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 3.1.15, 3.1.16 6.31.6, 11.6.2 11.6.5, Cisco, file: 3.1.15, 3.1.16, 6.31.6, 11.6.2, 11.6.5.docx dated 28 March 2011

d. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 3.3.1-.9, 11.3.1, 11.5.2, 11.9.1-5, 11.9.8-9, Cisco, file: 3.3.1-.9, 11.3.1, 11.5.2, 11.9.1-5 and 11.9.8-9.docx Dated 6 April 2011
e. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5, 3.4.6, Cisco, file: 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5, 3.4.6.docx dated 29 March 2011
f. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 3.5.1-3.5.12, 5.4.1(4a)-5.4.1(4c), 5.8, 6.14, 6.26, 6.31.11, 6.31.12, 11.3.2, Cisco, file: 3.5.1-3.5.12, 5.4.1(4a)-5.4.1(4c), 5.8, 6.14, 6.26, 6.31.11, 6.31.12, 11.3.2, 11.5.1.docx dated 4 April 2011
g. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 3.6.1, 3.6.2, Cisco, file: 3.6.1, 3.6.2.docx dated 5 April 2011
h. [ASA 8.3 Common Criteria Detailed Test Plan Test Cases 3.6.3, 3.6.6, Cisco, file: 3.6.3, 3.6.6.docx dated 5 April 2011
i. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 3.6.4, 3.6.5, Cisco, file: 3.6.4, 3.6.5.docx dated 4 April 2011
j. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 3.6.7, 3.6.8, Cisco, file: 3.6.7, 3.6.8.docx dated 28 March 2011
k. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 5.1.1 (1 a.), 5.1.2 (1 b.), 5.1.3. (1 c.), 5.1.4. (1 d.), 5.1.5 (1 e.), 5.1.6 (1 f.), 5.3.1 (3 a.), 5.3.2 (3 b.), 5.3.3 (3 c.), 5.7 (7.), 5.9 (9.), 5.10 (10.), 6.4.1 (4. a.), 6.4.2 (4. b.), 6.5.1 (5a), 6.5.2 (5b), 6.7.2 (7b), 6.8.1 (8. a.), 6.8.2 (8b), Cisco, file: 5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.3.1, 5.3.2, 5.3.3, 5.7, 5.9, 5.10, 6.4.1, 6.4.2, 6.5.1, 6.5.2, 6.7.2, 6.8.1, 6.8.2.docx dated 6 April 2011
l. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 6.15, 6.16, Cisco, file: 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 6.15, 6.16.docx dated 4 April 2011
m. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 5.4.5, Cisco, file: 5.4.5.docx dated 28 March 2011
n. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 5.5.1, 5.5.2, 6.1, 6.2, 6.3.1, 6.3.2, 6.6.1, 6.6.2, 6.10, 6.11, 6.12, 6.13, 6.24, 11.9.6, 11.10.2, 11.12.6.1, Cisco, file: 5.5.1, 5.5.2, 6.1.1 to 6.13, 6.24, 11.9.6, 11.10.2, 11.12.6.1.docx dated 4 April 2011
o. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 5-F, 5-G, 5-H, 5-I, 5-J, 5-P, 5-T, 5-U, 12, Cisco, file 5f, 5h, 5i, 5j, 5p, 12.docx dated 14 April 2011
p. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 5R-A, 5R-B, 5R-C, 5R-D, 5R-E, 5R-F, 5R-G, 5S-A, 5S-B, 5S-C, 5S-D, Cisco, file 5r, 5s.docx dated 20 April 2011
q. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 6.31.1, 6.31.2, 6.31.5, 6.31.7, 6.31.9, Cisco, file: 6.31.1, 6.31.2, 6.31.5, 6.31.7, 6.31.9.docx dated 4 April 2011
r. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 10-A, 10-B, 10-C, 10-D, 10-E, 10-F, 10-G, 10-H, 11-A, 11-B, Cisco, file 10A, 10B, 10C, 10D, 10E, 10F, 10G, 10H, 11A, 11B.docx dated 6 April 2011

s. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 11.1.3, 11.2.1, 11.2.3.2, 11.2.3.3, 11.2.3.4, 11.2.3.5, 11.2.3.6, 11.2.3.7, 11.11.5, Cisco, file: 11.1.3, 11.2.1, 11.2.3.2, 11.2.3.3, 11.2.3.4, 11.2.3.5, 11.2.3.6, 11.2.3.7, 11.11.5.docx dated 6 April 2011
t. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 29, 25.1A, 25.1B, Cisco, file 29, 25.1.docx dated 3 March 2011
u. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 303048.8.1 (Td9303999c), Cisco, file: fn.vpn_author.303048.8.1.docx dated 28 March 2011
v. ASA 8.3 Common Criteria Detailed Test Plan Test Cases syslog 113006, Cisco, file: syslog 113006.docx dated 28 March 2011
w. ASA 8.3 Common Criteria Detailed Test Plan Test Cases syslog 716040, Cisco, file: syslog 716040.docx dated 28 March 2011
x. ASA 8.3 Common Criteria Detailed Test Plan Test Cases syslogs 713082, 713198, 713215, 717009, Cisco, file: syslogs-713082-713198-713215-717009.docx dated 28 March 2011
y. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 5a, 25.2a, 25.2b, 25.2c, 25.2d, 25.2e, 25.2f, 25.2g, 25.2h, 25.2i, 25.2j, 25.2k, 25.2l, 25.4, 26.1, 26.2, 26.3, 26.4, 26.5, 26.6, Cisco, file TC 5a, 25.2a, 25.2b, 25.2c, 25.2d, 25.2e, 25.2f, 25.2g, 25.2h, 25.2i, 25.2j, 25.2k, 25.4, 26.1, 26.2, 26.3, 26.4, 26.5, ~1.docx dated 22 April 2011
z. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.5, 11.4.6, 11.4.7, 11.4.8, 11.4.9, Cisco, file TC 11.4.1 11.4.2 11.4.3 11.4.4 11.4.5 11.4.6 11.4.7 11.4. 8 11.4.9.docx dated 28 April 2011
aa. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 25.5.1, 25.5.2, 27.1, 27.2, 27.3, 27.4, 27.5, 35, Cisco, file TC 25.5.1, 25.5.2, 27.1, 27.2, 27.3, 27.4, 27.5, 35 - new test cases.docx dated 13 April 2011
bb. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 25.11, 25.12, 25.13, 25.15, Cisco, file TC 25.11 25.12, 25.13, 25.15.docx dated 27 April 2011
cc. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 37, Cisco, file TC 37.docx dated 26 April 2011
dd. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 38, Cisco, file TC 38.docx dated 26 April 2011
ee. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 39, Cisco, file TC 39.docx dated 18 April 2011
ff. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 40, Cisco, file TC 40.docx dated 15 April 2011
gg. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 41, 43, Cisco, file TC 41, 43.docx dated 15 April 2011
hh. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 42, Cisco, file TC 42.docx dated 15 April 2011
ii. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 44, Cisco, file TC 44.docx dated 26 April 2011

jj. ASA 8.3 Common Criteria Detailed Test Plan Test Cases 45, Cisco, file TC 45.docx dated 26 April 2011

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 Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform, Version 2.0, June 13, 2011.

7.1 Developer Testing

At EAL4, testing must demonstrate correspondence between the tests and the functional specification. The vendor testing addressed each of the security functions identified in the ST and interfaces in the design. These security functions include:

1. VPN and/or Firewall Information Flow Control
2. Audit
3. Identification & Authentication
4. Management
5. Cryptography

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the Common Criteria Guide, ran 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 testing focused on testing boundary conditions not tested by Cisco. The evaluation team tested combinations of the information flow policies that Cisco did not test. For vulnerability testing the evaluation team performed port and vulnerability scanning as well as other team developed tests.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform including:

- Hardware Models - Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580-20, and 5580-40
- Software Versions - Cisco ASA Release 8.3.2, Cisco AnyConnect Release 2.5, Cisco VPN Client Release 5.0, Cisco Adaptive Security Device Manager (ASDM) 6.3.2

To use the product in the evaluated configuration, the product must be configured as specified in the **Cisco Adaptive Security Appliances (ASA) Firewall and Virtual**

Private Network (VPN) Platform Common Criteria Operational User Guidance and Preparative Procedures 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.2 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 3.1 rev 3 and CEM version 3.1 rev 3. The evaluation determined the Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.2 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 Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform 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 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 and a detailed design document. 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.

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 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.

9.4 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 ALC evaluation also 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.

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.

9.5 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. The evaluation team re-ran the entire 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.

9.6 Vulnerability Assessment Activity (VAN)

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 evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests. The evaluation team's analysis included a comprehensive review of publicly-reported vulnerabilities in this and related products. This search did not uncover any vulnerabilities.

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 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 validation team considers the evaluated subset of product functions to be consistent with the product's intended purpose and mode of operation. The rationale for excluded features is plausible and introduces no unreasonable constraints.

The evaluation team observed that the vendor's security tests are predominantly manual and apparently not closely integrated with the extensive automated testing performed as a routine part of product development. While these evaluated tests are sufficient to satisfy Common Criteria requirements, the validation team recommends a closer integration in future efforts, in order to improve test integration and provide greater test coverage.

The following is a warning for the administrator. The shutdown of audit function is recorded in the audit trail indirectly. The TSF denies new connections whenever the TSF cannot send audit records to the syslog server in the operational environment. This includes both situations where the network connection is lost and situations where audit is shutdown manually. The syslog trail shows when the TSF re-establishes the connection with the syslog server and begins allowing new connections. The ASDM shows additional detail including: the loss of connection to the syslog server, when the TSF re-establishes the

connection, and re-enabling of audit in the manual case. See *Platform Preparative Procedures & Operational User Guide* section Monitoring & Maintenance for additional details

Although the vendor apparently maintains a significant internal organization responsible for vulnerability analysis and flaw remediation, the evaluation team was not provided access to any of that organization's personnel nor to the vulnerability reports and analysis performed therein. Again, while the materials provided are sufficient to satisfy the conformance requirements for vulnerability analysis and flaw remediation, the validation team considers the lack of access a lost opportunity to assess and describe the details of analysis and remediation work performed by the vendor.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform Target Security Target, Version 0.18, July 2011*.

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 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] 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.

[6] Science Applications International Corporation. *Evaluation Technical Report for the Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform Part 2 (Proprietary)*, Version 2.0, June 13, 2011.

[7] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform, ETR Part 2 Supplement (SAIC and Cisco Proprietary)*, Version 2.0, June 13, 2011.

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

[10] Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform Security Target, Version 0.18, July 2011.