National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 94002, USA

Cisco Adaptive Security Appliances and ASA Virtual 9.6

Report Number: CCEVS-VR-10759-2017
Dated: April 4, 2017
Version: 1.0

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Marybeth Panock
Kenneth Stutterheim
The Aerospace Corporation

Common Criteria Testing Laboratory

Tammy Compton
Ed Morris
Cornelius Haley
Chris Keenan
Catherine Sykes
Khai Van
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Architectural Information 4
3.1 TOE Evaluated Platforms 4
3.2 TOE Architecture 5
3.3 Physical Boundaries 5
4 Security Policy 7
4.1 Security Audit 7
4.2 Cryptographic Support 7
4.3 Full Residual Information Protection 7
4.4 Identification and Authentication 7
4.5 Security Management 8
4.6 Protection of the TSF 8
4.7 TOE Access 9
4.8 Trusted Path/Channels 9
4.9 Filtering 9
5 Assumptions 10
6 Clarification of Scope 11
7 Documentation 12
8 IT Product Testing 13
8.1 Developer Testing 13
8.2 Evaluation Team Independent Testing 13
8.3 Test Configuration 13
9 Evaluated Configuration 15
10 Results of the Evaluation 16
10.1 Evaluation of the Security Target (ASE) 16
10.2 Evaluation of the Development (ADV) 16
10.3 Evaluation of the Guidance Documents (AGD) 16
10.4 Evaluation of the Life Cycle Support Activities (ALC) 17
10.5 Evaluation of the Test Documentation and the Test Activity (ATE) 17
10.6 Vulnerability Assessment Activity (VAN) 17
10.7 Summary of Evaluation Results 17
11 Validator Comments/Recommendations 18
12 Annexes 19
13 Security Target 20
14 Glossary 21
15 Acronym List 22
16 Bibliography 23

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 and ASA Virtual 9.6 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 Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in March 2017. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated detailed test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements as defined in the Collaborative Protection Profile for Network Devices, version 1.0, February 27, 2015, Collaborative Protection Profile for Stateful Traffic Filter Firewalls, version 1.0, 27 February 2015 and VPN Gateway Extended Package, version 2.0, 01 December 2015.

The Target of Evaluation (TOE) is the Cisco Adaptive Security Appliances and ASA Virtual Version 9.6.

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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). 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, 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 Gossamer Security Solutions evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 1.

The technical information included in this report was obtained from the Cisco Adaptive Security Appliances and ASA Virtual Version 9.6 Security Target, Version 1.0, March 27, 2017 and analysis against additional evidence performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using Protection Profiles which contain Assurance Activities which are interpretation of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP 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 and ASA Virtual 9.6
Protection Profile	(Specific models identified in Section 3.1) Collaborative Protection Profile for Network Devices (NDcPP), version 1.0, February 27, 2015, Collaborative Protection Profile for Stateful Traffic Filter Firewalls, version 1.0, 27 February 2015 (FWcPP10) and VPN Gateway Extended Package, version 2.0, 01 December 2015 (VPNGWcEP20)
ST	Cisco Adaptive Security Appliances and ASA Virtual Version 9.6 Security Target, version 1.0, March 27, 2017
Evaluation Technical Report	Evaluation Technical Report for Cisco Adaptive Security Appliances and ASA Virtual Version 9.6, version 0.2, March 29, 2017 (Evaluation Sensitive)
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.

Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Marybeth Panock Kenneth Stutterheim

3 Architectural Information

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

The Cisco Adaptive Security Appliances TOE is a purpose-built network device firewall platform with VPN capabilities. The Cisco Adaptive Security Appliances Virtual running on UCS platform (TOE) is also a firewall platform with VPN capabilities.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

TOE Configuration	Hardware Configuration	Software Version
ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5508-X ASA 5516-X	The Cisco ASA 5500-X Adaptive Security Appliance provides high-performance firewall and VPN services and 4-8 Gigabit Ethernet interfaces, and support for up to 300 VPNs.	ASA release 9.6.2
ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	The Cisco ASA 5500-X Adaptive Security Appliance provides high-performance firewall and VPN services and 6-14 Gigabit Ethernet interfaces, and support for up to 5,000 VPNs.	ASA release 9.6.2
ASA 5585-X SSP-10 ASA 5585-X SSP-20 ASA 5585-X SSP-40 ASA 5585-X SSP-60	The Cisco ASA 5585 Adaptive Security Appliance provides high-performance firewall and VPN services and 6-16 Gigabit Ethernet interfaces, 2-10 10Gigabit Ethernet interfaces, and support for up to 10,000 VPNs.	ASA release 9.6.2
ASA Services Module (ASA-SM)	The Cisco Catalyst 6500 Series ASA Services Module supports up to: 20 Gbps maximum firewall throughput (max); 16 Gbps of maximum firewall throughput (multi-protocol); 300,000 connections per second; 10 million concurrent connections; 250 security contexts.	ASA release 9.6.2
ASAv	UCS B22 M3, B200 M3, B200 M4, B230 M2, B260 M4, B420 M3, B420 M4, B440 M2, B460 M4, C22 M3, C24 M3, C220 M3, C220 M4, C240 M3, C240 M4, C260 M2, C420 M3, C460 M2, C460 M4, E140S M1, E140S M2, E140D M1, E160D M2, E160D M1, E180D M2, E140DP M1, E160DP M1 including VM ESXi 5.5 and 6.0.	ASA release 9.6.2
ASDM	Included on all ASA models with ASA 9.6.2	Release 7.6

3.2 TOE Architecture

The TOE consists of hardware and software that provide connectivity and security services onto a single, secure device.

For firewall services, the ASA 5500-X Series, 5585-X Series, ASA-SM, and ASAv all provide 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.

The TOE also provides IPsec connection capabilities. All references within this ST to "VPN" connectivity refer to the use of IPsec tunnels to secure connectivity to and/or from the TOE, for example, gateway-to-gateway[1] VPN or remote access VPN. Other uses refer to the use of IPsec connections to tunnel traffic that originates from or terminates at the TOE itself, such as for transmissions from the TOE to remote audit/syslog servers, or AAA servers, or for an additional layer of security for remote administration connections to the TOE, such as SSH or TLS connections tunneled in IPsec.

The TOE protects itself from tampering and bypass by offering only a limited and controlled set of functions at each of its physical interfaces to its environment. Communication via those interfaces is either directed at the TOE for the purpose of administration or is directed through the TOE for communication among network devices. In both cases the TOE implements a set of policies to control the services available and those services are designed to protect and ensure the secure operation of the TOE.

3.3 Physical Boundaries

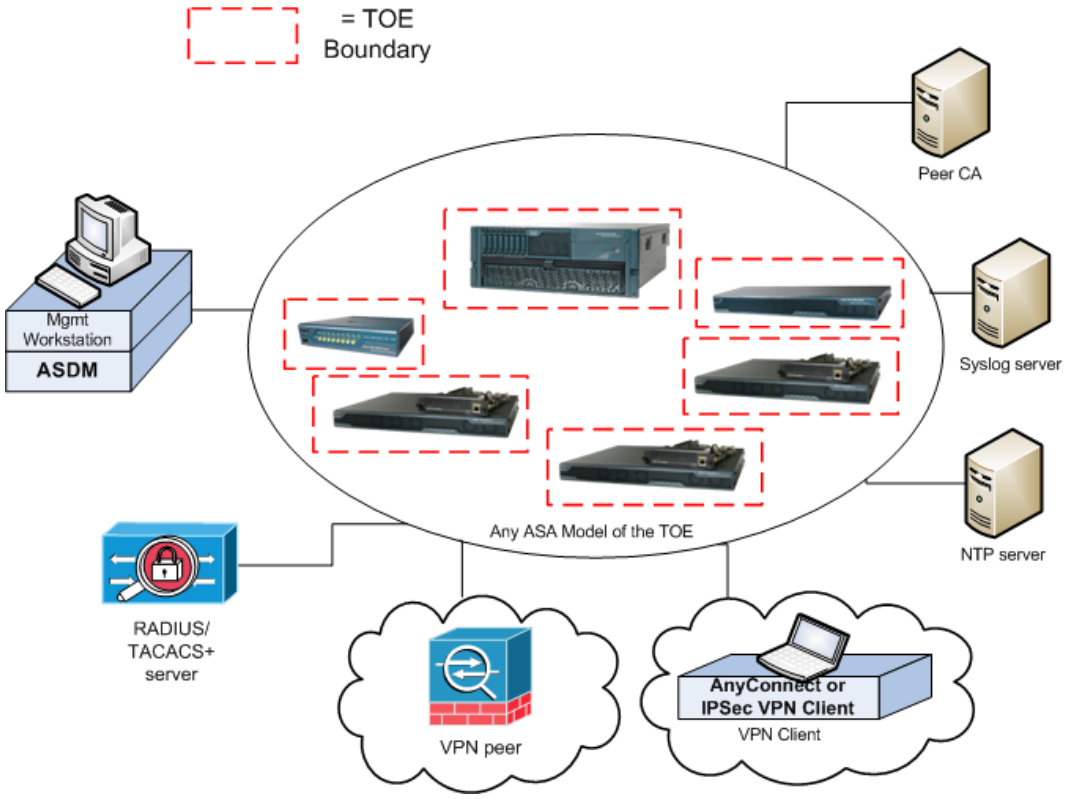
The TOE consists of one or more physical devices as specified in below and includes the Cisco ASA software, which in turn includes the ASDM software and for ASAv, the UCS platforms which includes the hypervisor. Each instantiation of the TOE has two or more network interfaces, and is able to filter IP traffic to and through those interfaces.

If the TOE is to be remotely administered, the management station must connect using SSHv2 over IPsec. When ASDM is used a remote workstation with a TLS-enabled browser must be available. A syslog server can also be used to store audit records, and the syslog server must support syslog over TLS or IPsec. The TOE is able to filter connections to/from these external using its IP traffic filtering, and can encrypt traffic where necessary using TLS and/or IPsec.

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.

Figure 1: Example TOE Deployment

[1] This is also known as site-to-site or peer-to-peer VPN.



The previous figure includes the following:

- Several examples of TOE Models
- VPN Peer (Operational Environment) or another instance of the TOE
- VPN Peer (Operational Environment) with Cisco VPN Client or AnyConnect Client
- Management Workstation (Operational Environment) with ASDM
- Remote Authentication Server (Operational Environment)
- NTP Server (Operational Environment)
- Peer CA (Operational Environment)
- Syslog server (Operational Environment)

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security Audit
2. Cryptographic support
3. Full Residual Information Protection
4. Identification and Authentication
5. Security Management
6. Protection of the TSF
7. TOE Access
8. Trusted Path/Channels
9. Filtering

4.1 Security Audit

The TOE provides auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are backed up over an encrypted channel to an external audit server.

4.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. The TOE provides cryptography in support of secure connections using IPsec and TLS, and remote administrative management via SSHv2 over IPsec, and TLS/HTTPS. The cryptographic random bit generators (RBGs) are seeded by an entropy noise source.

4.3 Full Residual Information Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

4.4 Identification and Authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the authorized administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec X509v3 certificate based authentication or pre-shared key methods.

The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI and GUI administrator interfaces. The TOE requires authorized

administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules. The TOE also implements a lockout mechanism if the number of configured unsuccessful login threshold has been exceeded.

The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console and HTTPS interfaces. The TOE optionally supports use of any RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE.

4.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 over IPsec or TLS/HTTPS session, or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users; all identification and authentication; all audit functionality of the TOE; all TOE cryptographic functionality; the timestamps maintained by the TOE; TOE configuration file storage and retrieval, and the information flow control policies enforced by the TOE including encryption/decryption of information flows for VPNs. The TOE supports an "authorized administrator" role, which equates to any account authenticated to an administrative interface (CLI or GUI, but not VPN), and possessing sufficient privileges to perform security-relevant administrative actions.

When an administrative session is initially established, the TOE displays an administrator-configurable warning banner. This is used to provide any information deemed necessary by the administrator. After a configurable period of inactivity, administrative sessions will be terminated, requiring administrators to re-authenticate.

4.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to authorized administrators. The TOE prevents reading of cryptographic keys and passwords.

Additionally TOE is not a general-purpose operating system and access to the TOE memory space is restricted to only TOE functions.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually, or can configure the TOE to use NTP to synchronize the TOE's clock with an external time source. Additionally, the TOE performs testing to verify correct operation of the appliance itself and that of the cryptographic module. Whenever any system failures occur within the TOE the TOE will cease operation.

4.7 TOE Access

When an administrative session is initially established, the TOE displays an administrator-configurable warning banner. This is used to provide any information deemed necessary by the administrator. After a configurable period of inactivity, administrator and VPN client sessions will be terminated, requiring re-authentication. The TOE also supports direct connections from VPN clients, and protects against threats related to those client connections. The TOE disconnects sessions that have been idle too long, and can be configured to deny sessions based on IP, time, and day, and to NAT external IPs of connecting VPN clients to internal network addresses.

4.8 Trusted Path/Channels

The TOE supports establishing trusted paths between itself and remote administrators using SSHv2 over IPsec for CLI access, and TLS/HTTPS for GUI/ASDM access. The TOE supports use of TLS and/or IPsec for connections with remote syslog servers. The TOE can use IPsec to encrypt connections with remote authentication servers (e.g. RADIUS). The TOE can establish trusted paths of peer-to-peer VPN tunnels using IPsec, and VPN client tunnels using IPsec or TLS. Note that the VPN client is in the operational environment.

4.9 Filtering

The TOE provides stateful traffic firewall functionality including IP address-based filtering (for IPv4 and IPv6) to address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance. Port and Address filtering can be configured to restrict the flow of network traffic between protected networks and other attached networks based on source and/or destination IP addresses or port. Stateful packet inspection is used to aid in the performance of packet flow through the TOE and to ensure that only packets are only forwarded when they're part of a properly established session. The TOE supports protocols that can spawn additional sessions in accordance with the protocol RFCs where a new connection will be implicitly permitted when properly initiated by an explicitly permitted session. System monitoring functionality includes the ability to generate audit messages for any explicitly defined (permitted or denied) traffic flow. TOE administrators have the ability to configure permitted and denied traffic flows, including adjusting the sequence in which flow control rules will be applied, and to apply rules to any network interface of the TOE.

The TOE also provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers as well as between remote VPN clients and the TOE. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using crypto map set.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Collaborative Protection Profile for Network Devices (NDcPP), version 1.0, February 27, 2015
- Collaborative Protection Profile for Stateful Traffic Filter Firewalls, version 1.0, 27 February 2015 (FWcPP10)
- Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway, version 2.0, 01 December 2015 (VPNGWcEP20)

That information has not been reproduced here and the NDcPP10/FWcPP10/VPNGWcEP20 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP10/FWcPP10/VPNGWcEP20 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Collaborative Protection Profile for Network Devices, collaborative Protection Profile for Stateful Traffic Filter Firewalls and VPN Gateway Extended Package and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP10/FWcPP10/VPNGWcEP20 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- Cisco Adaptive Security Appliance (ASA) 9.6 Preparative Procedures & Operational User Guide for the Common Criteria Certified configuration, Version 1.0, March 28, 2017

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report (FWcPP10/VPNGWcEP20) for Adaptive Security Appliances and ASA Virtual Version 9.6, Version 0.2, March 28, 2017 (DTR) which is summarized in the Assurance Activity Report.

8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

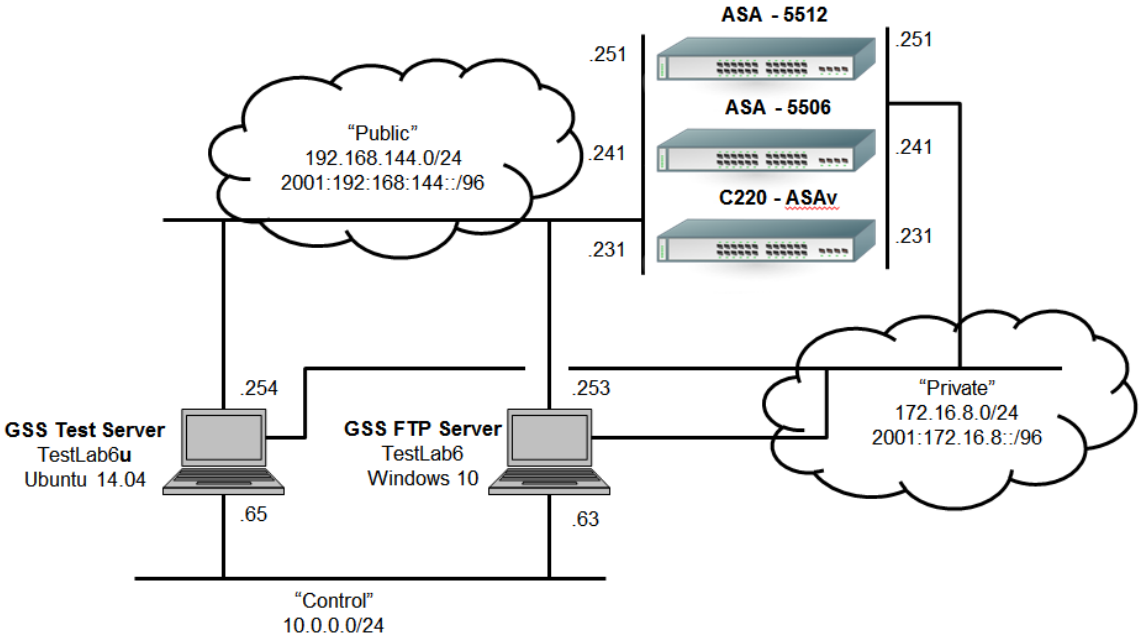
The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDcPP10/FWcPP10/VPNGWcEP20 including the tests associated with optional requirements.

8.3 Test Configuration

The evaluation team performed a set of tests based upon the assurance activities defined in the collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015, the collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 1.0, 27 February 2015 and the Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway, Version 2.0, 01 December 2015 (NDcPP10/FWcPP10/VPNGWcEP20).

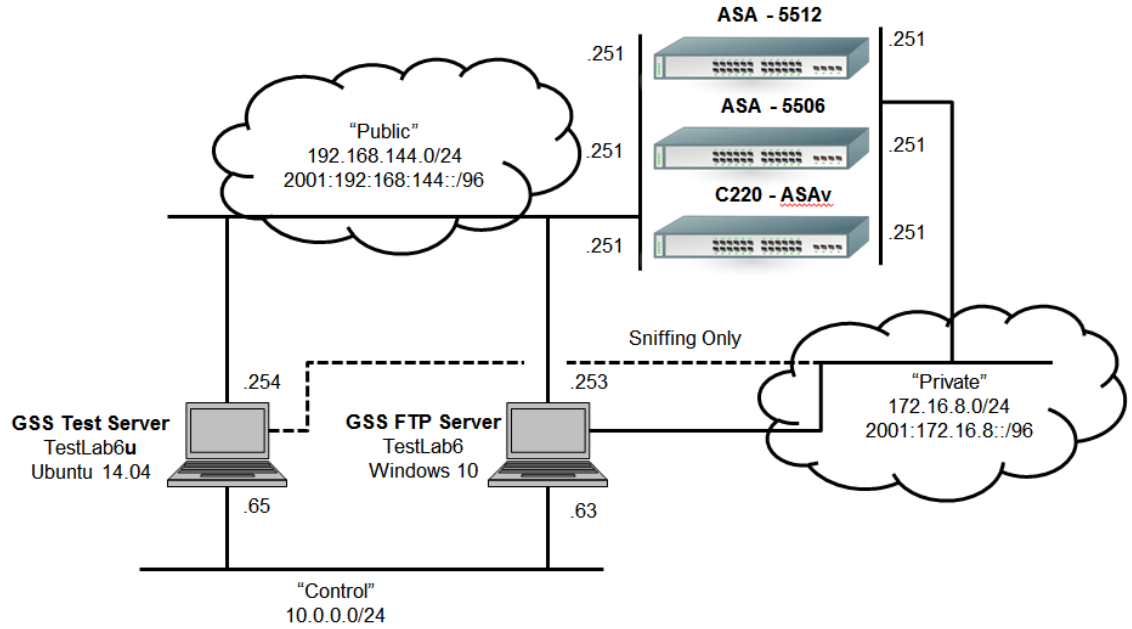
The following diagram indicates the test environment used during general testing and during IPsec testing.

General Testing Configuration



In addition, the evaluators used an alternate configuration during firewall testing.

Firewall Testing Configuration



9 Evaluated Configuration

The evaluated configuration consists of the following series and models:

- ASA 5500 Series (5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X) and (5512-X, 5515-X, 5525-X, 5545-X, 5555-X)
- ASA 5585 Series (5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40, 5585-X SSP-60)
- ASA Services Module (ASA-SM)[2]
- ASAv running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B22 M3, B200 M3, B200 M4, B230 M2, B260 M4, B420 M3, B420 M4, B440 M2, B460 M4, C22 M3, C24 M3, C220 M3, C220 M4, C240 M3, C240 M4, C260 M2, C420 M3, C460 M2, and C460 M4
- ASAv running on ESXi 5.5 or 6.0 on the E140S M1, E140S M2, E140D M1, E160D M2, E160D M1, E180D M2, E140DP M1, E160DP M1 installed on ISR[3]

The Cisco Adaptive Security Appliances that comprise the TOE have common hardware characteristics. These differing characteristics affect only non-TSF relevant functionality (such as throughput, processing speed, number and type of network connections supported, number of concurrent connections supported, and amount of storage) and therefore support security equivalency of the ASAs in terms of hardware.

[2] ASA-SM on Catalyst 6500 Series switches including 6503-E, 6504-E, 6509-E, and 6513-E in the operational environment.

[3] ISR is in the operational environment. Please see table 6 in section 1.3 for UCS-E and ISR compatibility.

10 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 assurance activities and 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 4 and CEM version 3.1 rev 4. The evaluation determined the Product Name TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Adaptive Security Appliances and ASA Virtual Version 9.6 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators 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.

10.2 Evaluation of the Development (ADV)

The evaluation team applied each 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 contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDcPP10/FWcPP10/VPNGWcEP20 related to the examination of the information contained in the TSS.

The validators 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.

10.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each 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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validators 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.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators 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.

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

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP10/FWcPP10/VPNGWcEP20 and recorded the results in an evaluation sensitive Test Report, summarized in the AAR.

The validators 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.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities and did not discover any public issues with the TOE.

The validators 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.

10.7 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 testing 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.

11 Validator Comments/Recommendations

Although the vendor provides multiple links to additional configuration guides, the validation team cautions the consumer to follow only the required elements contained within the configuration guide (as listed in Section 7 above) to ensure the product is deployed in accordance with the evaluated configuration. Note that the configuration guide includes instructions on how to install additional functionality, i.e. Firepower, which was not tested as part of the evaluation. As well, the list of item requirements for the Operational Environment as listed on pages 9 and 10 of the configuration guide may not have been tested as part of the evaluated configuration and no assumptions can be made nor inferred regarding their correct operation.

Note that for all versions of the product, especially virtualized versions, there are to be no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

The certified configuration places no restrictions on the use of the supported routing protocols; however evaluation of these protocols was beyond the scope of the Common Criteria product evaluation, so it is suggested that the consumer follow best practices for the secure usage of these protocols. For example, although the TOE supports dynamic establishment of secondary network sessions, other than TCP and UDP only FTP was claimed and tested.

IKEv2 must be used instead of IKEv1, and FIPS mode must be enabled in the evaluated configuration.

The Common Criteria certification did not evaluate any of the cryptographic functionality: MD5• RADIUS• SSHv2 which may be used, but only when tunneled in IPsec.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Cisco Adaptive Security Appliances and ASA Virtual 9.6 Security Target, Version 1.0, March 27, 2017*.

14 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.

15 Acronym List

CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PCL	Products Compliant List
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
VR	Validation Report

16 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] Collaborative Protection Profile for Stateful Traffic Filter Firewalls, version 1.0, 27 February 2015 (FWcPP10) and VPN Gateway Extended Package, version 2.0, 01 December 2015 (VPNGWcEP20)

[5] Cisco Adaptive Security Appliances and ASA Virtual 9.6 Security Target, Version 1.0, March 27, 2017 (ST)

[6] Assurance Activity Report (NDcPP10/FWcPP10/VPNGWcEP20) for Adaptive Security Appliances and ASA Virtual Version 9.6, Version 0.4, March 28, 2017 (AAR)

[7] Detailed Test Report (FWcPP10/VPNGWcEP20) for Adaptive Security Appliances and ASA Virtual 9.6, Version 0.2, March 28, 2017 (DTR)

[8] Evaluation Technical Report for Cisco Adaptive Security Appliances and ASA Virtual 9.6, Version 0.2, March 29, 2017 (ETR)

[9] Cisco Adaptive Security Appliance (ASA) 9.6 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration, Version 1.0, March 28, 2017