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 FirePOWER 6.1

Report Number: **CCEVS-VR-10768-2018**
Dated: **January 17, 2018**
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jean Petty
Brad O'Neill
Patrick Mallett, PhD.
Stelios Melachrinoudis
The MITRE Corporation

Kenneth Stutterheim
The Aerospace Corporation

Common Criteria Testing Laboratory

Cornelius Haley
Khai Van
Gossamer Security Solutions, Inc.
Catonsville, MD

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 FirePOWER 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 January 2018. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated 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 of the collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015 with the collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), Version 2.11, 15 June 2017.

The Target of Evaluation (TOE) is the Cisco FirePOWER 6.1.

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 technical information included in this report was obtained from the Cisco FirePOWER Version 6.1 Security Target, version 1.0, January 2, 2018 and analysis 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 the Common Evaluation Methodology (CEM) 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 FirePOWER 6.1 (Specific models identified in Section 3.1)
Protection Profile	collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015 with the collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), Version 2.11, 15 June 2017
ST	Cisco FirePOWER 6.1 Security Target, version 1.0, January 2, 2018
Evaluation Technical Report	Evaluation Technical Report for Cisco FirePOWER 6.1, version 0.3, January 3, 2018
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	Jean Petty, Brad O'Neill, Patrick Mallett, PhD., Stelios Melachrinoudis, The MITRE Corporation Kenneth Stutterheim, The Aerospace Corporation

3 Architectural Information

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

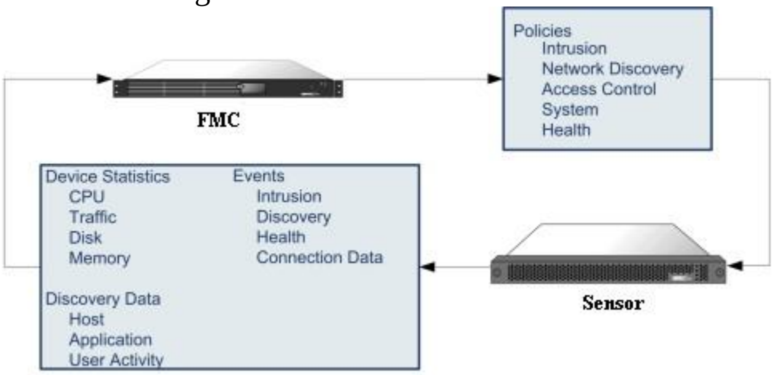
The TOE, sometimes referred to as Cisco FirePOWER NGIPS, provides advanced threat protection by integrating:

- Real-time contextual awareness - See and correlate extensive amounts of event data related to IT environments—applications, users, devices, operating systems, vulnerabilities, services, processes, network behaviors, files, and threats.
- Advanced threat protection - Protect against the latest threats. Discover, track, and block the progression of suspect files and malware to prevent the spread of outbreaks and reinfection.

A FMC is a fault-tolerant, purpose-built network appliance that provides a centralized management console and database repository for the FirePOWER System deployment. Administrators can also deploy 64-bit virtual FirePOWER Management Centers (FMCv) as ESXi 5.5 or 6.0 hosts using the VMware vSphere Hypervisor. The FMC is a key component in the Cisco NGIPS system. Administrators can use the FMC to manage the full range of Sensors that comprise the Cisco NGIPS system, and to aggregate, analyze, and respond to the threats they detect on their network. By using the FMC to managed Sensors, administrators can:

- Configure policies for all Sensors from a single location, making it easier to change configurations.
- Install various types of software updates on Sensors.
- Push policies to managed Sensors and monitor their health status from the FMC.

The FMC aggregates and correlates intrusion events, anomaly, network discovery information, and Sensor performance data, allowing administrators to monitor the information the Sensors are reporting in relation to one another, and to assess the overall activity occurring on their network. The following illustration lists what is transmitted between a FMC and its managed Sensors.



Cisco FirePOWER 7000, 8000, and AMP Series appliances are physical devices purpose-built for the Cisco NGIPS System. The Sensors have a range of throughputs, but share most of the same capabilities. The administrators can also deploy NGIPSv (a 64-bit virtual device on an ESXi 5.5 or 6.0 host) using the VMware vSphere Hypervisor on the hardware platforms as specified below in section 3.1. The administrators can configure the Sensors in either a passive or inline deployment. In a passive deployment, the Sensor monitors traffic flowing across a network using a switch SPAN or mirror port. However, when configured in a passive deployment, the TOE cannot take certain actions such as blocking or shaping traffic. In an inline IPS deployment, the Sensor operates as a bump in the wire and is transparent (i.e., no IP address) on a network segment. The Sensor can be configured to drop or alter packets, if necessary, in addition to generating alerts.

The TOE hardware appliances are purpose-built running on top of a customized, hardened Linux kernel. The hardware and operating system on which the Cisco NGIPS System software operates provide the support necessary for the software applications to exist as processes and to access necessary disk, memory, and network connection resources. The appliance hardware, the underlying operating systems, embedded database, and third-party applications installed on the appliances provide support for the security functions and associated security management of the TOE. The TOE virtual appliance consists of the same virtual components (described above) running on VMware ESXi 5.5 and 6.0 hypervisor and the underlying UCS model hardware.

3.1 TOE Evaluated Platforms

TOE Configuration	**Hardware Configurations**	**Software Version**
Cisco FirePOWER 7010 Cisco FirePOWER 7020 Cisco FirePOWER 7030 Cisco FirePOWER 7050 Cisco FirePOWER 7110 Cisco FirePOWER 7115 Cisco FirePOWER 7120 Cisco FirePOWER 7125 	The Cisco FirePOWER 7000 Series provides high-performance IPS services including up to 12 monitoring interfaces, and up to 1.25 Gbps throughput.	Release 6.1
Cisco FirePOWER 8120 Cisco FirePOWER 8130 Cisco FirePOWER 8140 Cisco FirePOWER 8250 Cisco FirePOWER 8260 Cisco FirePOWER 8270 Cisco FirePOWER 8290 Cisco FirePOWER 8350 Cisco FirePOWER 8360 Cisco FirePOWER 8370 Cisco FirePOWER 8390 	The Cisco FirePOWER 8000 Series provides high-performance IPS services including up to 14 monitoring interfaces, and up to 60 Gbps throughput.	Release 6.1
Cisco FirePOWER AMP 7150 Cisco FirePOWER AMP 8050 Cisco FirePOWER AMP 8150 Cisco FirePOWER AMP 8350 Cisco FirePOWER AMP 8360	The Cisco FirePOWER AMP Series provides high-performance IPS services including up to 28 monitoring interfaces, and up to 20 Gbps throughput.	Release 6.1

Cisco FirePOWER AMP 8370 Cisco FirePOWER AMP 8390 		
FMCv **NGIPSv**	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.	Release 6.1

3.2 TOE Architecture

The system architecture can be depicted as follows:

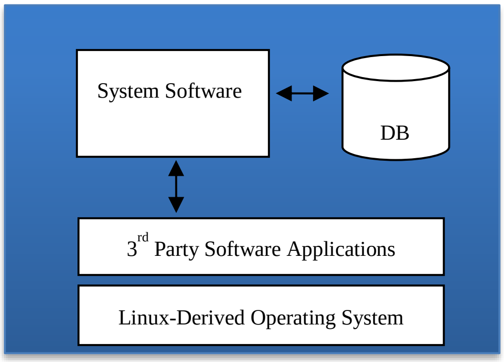

System Software
DB
3rd Party Software Applications
Linux-Derived Operating System

Figure 1: System Architecture

The TOE main subsystems are summarized as followed:

- System Software – The TOE main processes that provide the majority of the security management functions— including the SF CLI and web GUI—and proprietary algorithms to analyze, correlate, and display intrusion events.
- Database (DB) – The TOE contains a database which acts as the data repository for audit records, system event data, user account data, TOE and system configuration data. The system events sent from the managed Sensors are also stored in the database of the FMC.
- 3rd Party Software Applications – The TOE uses third party software processes and daemons to provide support to the 3D System Software subsystem. The supports include providing the underlying security protocols to protect the management communications (e.g., OpenSSH), FIPS-certified cryptographic algorithms (e.g., OpenSSL), web server to host web GUI (e.g., Tomcat Apache), auditing capability (e.g., auditd, syslog-ng), other network services (e.g., ntp, net-snmp, dhcp), etc.
- Linux-Derived Operating System – The TOE uses a customized Linux kernel to provide domain separation, memory management, disk access, file I/O, network stacks (IPv4/IPv6), and communications with the underlying hardware including the network

interface cards. Only the services and packages required by the TOE for secure operation are enabled.

The TOE is composed of subsystems that implement security and management functions. For example there are subsystems dedicated to SNMP traps, web, and CLI management. There are also subsystems dedicated to the IPv4 and IPv6 network stacks as well as the applicable network protocols and switching, routing, etc.
From a security perspective, the TOE includes a cryptographic module that supports SSH, TLS, and HTTPS (HTTP over TLS) and digital signatures used to protect the available remote management and cryptographic hash to enable secure update capabilities of the TOE. The TOE also implements a wide range of non-security related functions such as network switching protocols and high-availability.

The hardware components in the TOE have the following distinct characteristics:

Model	**7010**	**7020**	**7030**	**7050**
Processor	Intel Atom D2xxx Series	Intel Atom D2xxx Series	Intel Atom D2xxx Series	Intel Pentium B9xx Series
IPS Throughput	50 Mbps	100 Mbps	250 Mbps	500 Mbps
Monitoring Interface	(8) 1-Gbps copper	(8) 1-Gbps copper	(8) 1-Gbps copper	(8) 1-Gbps copper
Management Interface	RJ45	RJ45	RJ45	RJ45
Management Interface Speed	10/100/1000	10/100/1000	10/100/1000	10/100/1000
Memory (RAM)	4 GB	4 GB	4 GB	4 GB
Cooling Fans	2	2	2	2

Model	**7110**	**7115**	**7120**	**7125**
Processor	Intel Xeon 3400 Series	Intel Xeon 3400 Series	Intel Xeon 3400 Series	Intel Xeon 3400 Series
IPS Throughput	500 Mbps	750 Mbps	1 Gbps	1.25 Gbps
Monitoring Interface	(8) 1-Gbps copper; (8) 1-Gbps short-reach fiber	(12) total – (4) 1-Gbps copper; (8) SFP sockets	(8) 1-Gbps copper; (8) 1-Gbps short-reach fiber	(12) total – (4) 1-Gbps copper; (8) SFP sockets
Management Interface	RJ45	RJ45	RJ45	RJ45
Management Interface Speed	10/100/1000	10/100/1000	10/100/1000	10/100/1000
Memory (RAM)	16 GB	16 GB	16 GB	16 GB
Cooling Fans	5	5	5	5

Model	**8120**	**8130**	**8140**
Processor	Intel Xeon 5600 Series	Intel Xeon 5600 Series	Intel Xeon 5600 Series
IPS Throughput	2 Gbps	4 Gbps	6 Gbps

Monitoring Interface	(4) 1-Gbps copper;
	(4) 1-Gbps fiber;
	(2) 10-Gbps SR;
	(2) 10-Gbps LR
		(4) 1-Gbps copper;
		(4) 1-Gbps fiber;
		(2) 10-Gbps SR;
		(2) 10-Gbps LR
			(4) 1-Gbps copper;
			(4) 1-Gbps fiber;
			(2) 10-Gbps SR;
			(2) 10-Gbps LR

Management Interface	RJ45	RJ45	RJ45
Management Interface Speed	10/100/1000	10/100/1000	10/100/1000
Memory (RAM)	24 GB	24 GB	24 GB

Cooling Fans	10	10	10

Model	**8250**	**8260**	**8270**	**8290**
Processor	Intel Xeon 5600 Series	Intel Xeon 5600 Series	Intel Xeon 5600 Series	Intel Xeon 5600 Series
IPS Throughput	10 Gbps	20 Gbps	30 Gbps	40 Gbps

Monitoring Interface	(4) 1-Gbps copper;
	(4) 1-Gbps fiber;
	(2) 10-Gbps SR;
	(2) 10-Gbps LR;
	(2) 40-Gbps SR
		(4) 1-Gbps copper;
		(4) 1-Gbps fiber;
		(2) 10-Gbps SR;
		(2) 10-Gbps LR;
		(2) 40-Gbps SR
			(4) 1-Gbps copper;
			(4) 1-Gbps fiber;
			(2) 10-Gbps SR;
			(2) 10-Gbps LR;
			(2) 40-Gbps SR
				(4) 1-Gbps copper;
				(4) 1-Gbps fiber;
				(2) 10-Gbps SR;
				(2) 10-Gbps LR;
				(2) 40-Gbps SR

Management Interface	RJ45	RJ45	RJ45	RJ45
Management Interface Speed	10/100/1000	10/100/1000	10/100/1000	10/100/1000
Memory (RAM)	48 GB	96 GB	144 GB	192 GB
Cooling Fans	6	12	18	24

Model	**8350**	**8360**	**8370**	**8390**
Processor	Intel Xeon E5 2600 Series	Intel Xeon 5600 Series	Intel Xeon 5600 Series	Intel Xeon 5600 Series
IPS Throughput	15 Gbps	30 Gbps	45 Gbps	60 Gbps

Monitoring Interface	(4) 1-Gbps copper;
	(4) 1-Gbps fiber;
	(2) 10-Gbps SR;
	(2) 10-Gbps LR;
	(2) 40-Gbps SR
		(4) 1-Gbps copper;
		(4) 1-Gbps fiber;
		(2) 10-Gbps SR;
		(2) 10-Gbps LR;
		(2) 40-Gbps SR
			(4) 1-Gbps copper;
			(4) 1-Gbps fiber;
			(2) 10-Gbps SR;
			(2) 10-Gbps LR;
			(2) 40-Gbps SR
				(4) 1-Gbps copper;
				(4) 1-Gbps fiber;
				(2) 10-Gbps SR;
				(2) 10-Gbps LR;
				(2) 40-Gbps SR

Management Interface	RJ45	RJ45	RJ45	RJ45
Management Interface Speed	10/100/1000	10/100/1000	10/100/1000	10/100/1000
Memory (RAM)	128 GB	256 GB	384 GB	512 GB
Cooling Fans	6	12	18	24

Model	**AMP7150**	**AMP8050**	**AMP8150**	**AMP8350**
Processor	Intel Xeon 3400 Series	Intel Xeon 5600 Series	Intel Xeon 5600 Series	Intel Xeon E5 2600 Series
AMP Throughput	500 Mbps	1 Gbps	2 Gbps	5 Gbps
Max Monitoring Interface	12	12 (3 x 4-Port RJ45 Netmods)	12 (3 x 4-Port RJ45 Netmods)	28 (7 x 4-Port RJ45 Netmods)
Management Interface	RJ45	RJ45	RJ45	RJ45
Management Interface Speed	10/100/1000	10/100/1000	10/100/1000	10/100/1000
Solid State Drive (SSD) Capacity	120 GB	400+ GB	400 GB	400+ GB
Cooling Fans	5	10	10	6

Model	**AMP8360**	**AMP8370**	**AMP8390**
Processor	Intel Xeon 5600 Series	Intel Xeon 5600 Series	Intel Xeon 5600 Series
AMP Throughput	10 Gbps	15 Gbps	20 Gbps
Max Monitoring Interface	24 (6 x 4-Port RJ45 Netmods)	20 (5 x 4-Port RJ45 Netmods)	16 (4 x 4-Port RJ45 Netmods)
Management Interface	RJ45	RJ45	RJ45
Management Interface Speed	10/100/1000	10/100/1000	10/100/1000
Solid State Drive (SSD) Capacity	800+ GB	1200+ GB	1600+ GB
Cooling Fans	12	18	24

Model	**FS750**	**FS1500**	**FS2000**	**FS3500**	**FS4000**
Processor	Intel Xeon E3 1200 Series	Intel Xeon E5600 Series	Intel Xeon E5 2600 Series	Intel Xeon E5600 Series	Intel Xeon E5 2600 Series
Maximum Number of Sensors Managed	10	35	70	150	300
Maximum Number of IPS Events	20 Million	30 Million	60 Million	150 Million	300 Million
Event Storage	100 GB	125 GB	1.8 TB	400 GB	4.8 TB
Maximum Flow Rate	2,000 fps	6,000 fps	12,000 fps	10,000 fps	20,000 fps
Maximum Network Map (hosts/users)	2,000/2,000	50,000/50,000	150,000/150,000	300,000/300,000	600,000/600,000
Network Interfaces	2 x 1Gbps	2 x 1Gbps	2 x 1Gbps 2 x 10Gbps	2 x 1Gbps	2 x 1Gbps 2 x 10Gbps
The same FirePOWER image runs on all of the model platforms identified in this table.					

The underlying UCS platforms 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 FMCv and NGIPSv in terms of hardware.

The UCS hardware components in the TOE have the following distinct characteristics:

Model	B200 M3	B200 M4	B420 M4	B420 M3	B260 M4	B460 M4
Number of Processors	2	2	2 or 4	2 or 4	2	4
Processor	Intel Xeon E5-2600 product families	Intel Xeon E5-2600 processor product family	Intel Xeon E5-4600 processor product family	Intel Xeon E5-4600 processor product families	Intel Xeon E7 processor product family	Intel Xeon E7 processor product family
Form factor	Half-width blade	Half-width blade	Full-width blade	Full-width blade	Full-width blade	Full-width Double-high blade
Maximum Memory	768 GB, 24 DIMMs	768 GB, 24 x DDR4 DIMMs	3.0 TB, 48 DIMMs	1.5 TB, 48 DIMMs	3.0 TB, 48 DIMMs	6.0 TB, 96 DIMMs
Disk Space	2.0 TB	3.2 TB	4.8 TB	4.0 TB	2.4 TB	4.8 TB
Max I/O per blade	80 Gbps (2 x 40 Gbps)	80 Gbps (2 x 40 Gbps)	160 Gbps	160 Gbps (4 x 40 Gbps)	160 Gbps (4 x 40 Gbps)	160 Gbps (4 x 40 Gbps)

Model	B22 M3	B230 M2	B440 M2
Number of Processors	2	2	2 or 4
Processor	Intel Xeon E5-2400 product family	Intel Xeon E7-2800 or E7-8800 series processor	Intel Xeon E7-4800 or E7-8800 series processor
Form factor	Half-width blade	Half-width blade	Full-width blade
Maximum Memory	384 GB of RAM with 12 DIMM slots	512 GB of RAM with 32 DIMM slots	1 TB of RAM with 32 DIMM slots
Disk Space	1.0 TB	400 GB	900 GB
Max I/O per blade	80 Gbps	80 Gbps (2 x 40 Gbps)	160 Gbps

Model	C22 M3	C24 M3	C220 M3	C220 M4	C240 M3
Number of Processors	1 or 2	1 or 2	2	2	2
Processor	Intel Xeon E5-2400 processor product family	Intel Xeon E5-2400 processor product family	Intel Xeon E5-2600 processor product families	Intel Xeon E5-2600 processor product family	Intel Xeon E5-2600 processor product families
Form factor	1 RU	2 RU	1 RU	1 RU	2 RU
Memory	384 GB, 12 x DDR3 DIMMs	384 GB, 12 x DDR3 DIMMs	512 GB, 16 x DDR3 DIMMs	768 GB, 24 x DDR4 DIMMs	768 GB, 24 x DDR4 DIMMs
Disk Space	SFF- 8 TB	SFF- 16 TB	SFF- 9.6 TB	SFF - 12.8 TB	SFF- 28.8 TB

	LFF- 16 TB	LFF- 32 TB	LFF- 16 TB	LFF - 16 TB	LFF- 48 TB
I/O	2 x 1 Gb ports	2 x 1 Gb ports	2 x 1 Gb ports	2 x 1 Gb ports plus 1 x Modular LOM (MLOM)	4 x 1 Gb ports

Model	**C240 M4**	**C260 M2**	**C420 M3**	**C460 M2**	**C460 M4**
Number of Processors	2	2	2 or 4	2 or 4	2 or 4
Processor	Intel Xeon E5-2600 processor product family	Intel Xeon E7-2800 / 8800 processor product families	Intel Xeon E5-4600 processors product family	Intel Xeon E7-4800 / 8800 processor product families	Intel Xeon E7-4800 / 8800 processor product families
Form factor	2 RU	2 RU	2 RU	4 RU	4 RU
Memory	768 GB, 24 x DDR4 DIMMs	1 TB, 64 x DDR3 DIMMs	1.5 TB, 48 x DDR3 DIMMs	2 TB, 64 x DDR3 DIMMs	Up to 3 TB
Disk Space	SFF - 38.4 TB LFF - 48 TB	16 TB	16 TB	12 TB	12.8 TB
I/O	2 x 1 Gb ports plus 1 x Modular LOM (MLOM)	2 x 1 Gb ports 2 x 10 Gb SFP+ ports (optional)	4 x 1 Gb ports	2 x 1 Gb ports 2 x 10 Gb ports 2 x 10 Gb SFP+ ports	2 x 1 Gb ports 2 x 10 Gb ports

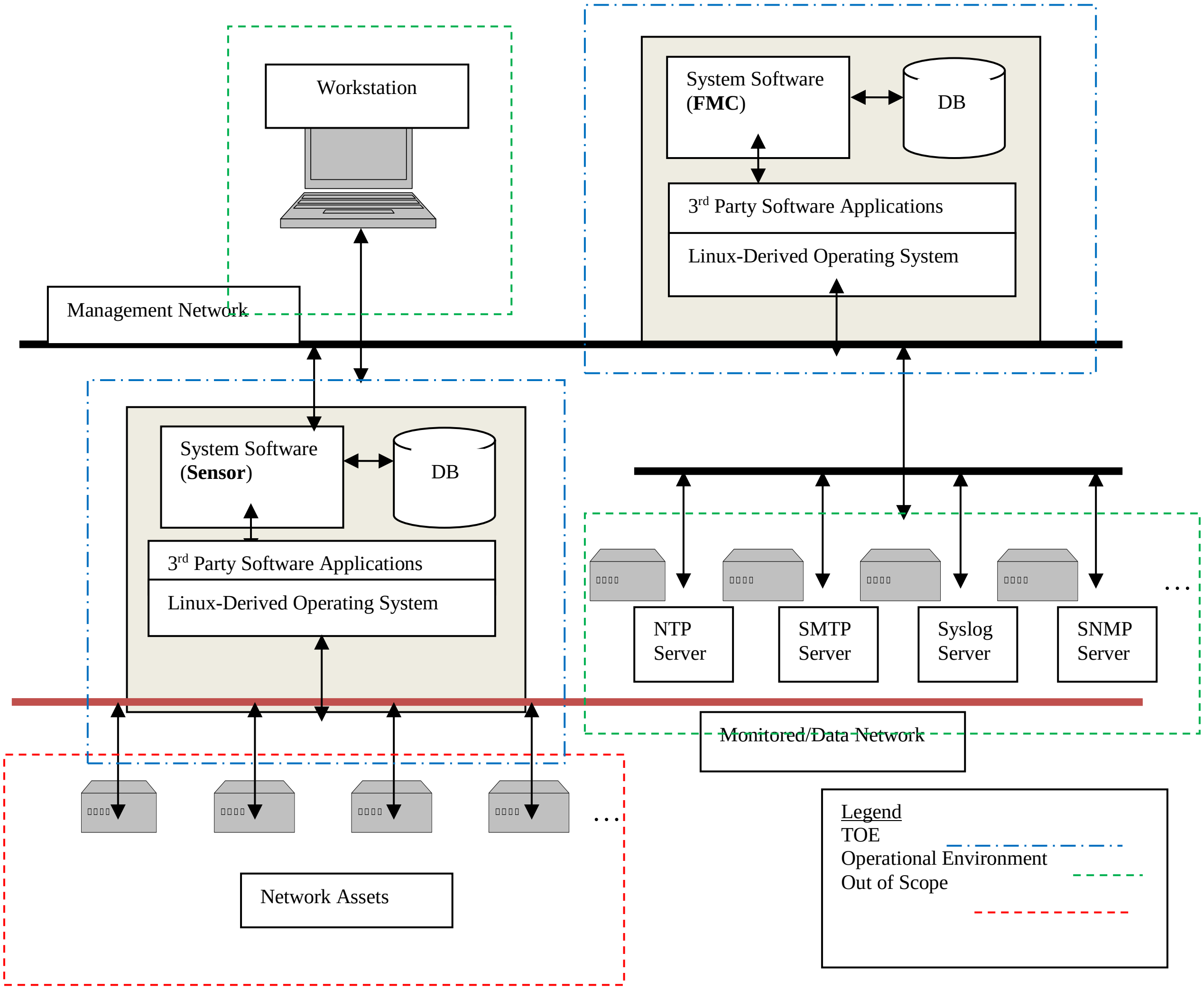
Model	**UCS E140S M1 and M2**	**UCS E140D M1 and E160D M2 & M1 E180D M2**	**UCS E140DP M1 and E160DP M1**
Number of Processors	4	4, 6, or 8	4 or 6
Processor	Intel Xeon processor E3-1100 Series	Intel Xeon processor E5-2400 Series	Intel Xeon processor E5-2400 Series
Form factor	Single-Wide Blade	Double-Wide Blades	Double-Wide Blades with PCIe Cards
Memory	8 GB (default) and up to 16 GB (two 8-GB DIMMs)	8 GB (default) and up to 48 GB (three 16-GB DIMMs)	8 GB (default) and up to 48 GB (three 16-GB DIMMs)
Disk Space	Up to two: • 7200-RPM SATA: 1 TB • 10,000-RPM SAS: 900 GB • 10,000-RPM SAS SED: 600 GB	Up to three : • 7200-RPM SATA: 1 TB • 10,000-RPM SAS: 900 GB • 10,000-RPM SAS SED: 600 GB	Up to two: • 7200-RPM SATA: 1 TB • 10,000-RPM SAS: 900 GB • 10,000-RPM SAS SED: 600 GB

NICs	Two internal and one external Gigabit Ethernet ports	Two internal and two external Gigabit Ethernet ports	Two internal and two external Gigabit Ethernet ports

The evaluated product conforms to the NDcPP10/IPScEP211, the security claims focus on the TOE as a secure network infrastructure device and intrusion protection system. The security claims do not focus on any other functions provided by the TOE, such as controlling the flow of network packets among the attached networks. Those functions have not been evaluated to ensure their correct operation.

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 to 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 previous figure includes the following:

- FMC and Sensor (TOE)
- Management Workstation (Operational Environment)
- NTP Server (Operational Environment)
- Syslog Server (Operational Environment)
- SMTP Server (Operational Environment)
- SNMP Server (Operational Environment)

The TOE may be accessed and managed through a PC or terminal in the operational environment which can be remote from or directly connected to the TOE. The TOE can be configured to synchronize its internal clock using an NTP server in the operational environment.

The TOE can be configured to communicate with SYSLOG servers in its environment to export audit data across trusted channels. The TOE can support interaction with SYSLOG servers in accordance with their respective protocols, including security capabilities where applicable.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security Management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels
8. Intrusion Prevention System

4.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events such as login attempts and management functions. The complete list of auditable events and contents is in TSS. The TOE can be configured to store the logs locally so they can be accessed by an administrator or alternately to send the logs to an external syslog server over a secure communication channel. The timestamp included in the audit content can be manually set or set by an external NTP server in the operational environment.

4.2 Cryptographic support

The TOE includes a cryptographic module that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including TLS, HTTPS, and SSH. The complete specification of algorithms, key sizes, and other attributes is in TSS.

4.3 Identification and authentication

The TOE requires administrators to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console as well as network accessible interfaces (SSHv2 and HTTPS) for remote interactive administrator sessions.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. All authorized TOE users must have a user account with security attributes that control the user’s access to TSF data and management functions. These security attributes include user name, password, and roles for TOE users. In addition, the TOE supports X.509v3 certificate authentication for the external syslog server.

Optionally, the TOE can be configured to utilize the services of trusted RADIUS and LDAP servers in the operational environment to support centralized user administration.

4.4 Security management

The TOE provides a web-based (using HTTPS) management interface for all TOE administration, including the IDS and access control rule sets, user accounts and roles, and audit functions. The ability to manage various security attributes, system parameters and all TSF data is controlled and limited to those users who have been assigned the appropriate administrative role.

The TOE also provides a command line interface (CLI) and shell access to the underlying operating system of the TOE components. The shell access must be restricted to off-line installation, pre-operational configuration, and maintenance and troubleshooting of the TOE. The CLI provides only a subset of the management functions provided by the web GUI and is only available on the Sensors. The use of the web GUI is highly recommended over the CLI.

Security management relies on a management workstation in the operational environment with a properly supported web browser or SSH client to access the management interfaces.

4.5 Protection of the TSF

The TOE implements features to protect itself to ensure the reliability and integrity of its security functionality. It protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability) or, if so configured, can utilize a trusted time server in the operational environment.

The TOE ensures that data transmitted between separate parts of the TOE are protected from disclosure or modification. This protection is ensured by transmission of data between the TOE components over a secure, TLS-protected tunnel.

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

4.6 TOE access

The TOE can be configured to display an informative advisory banner when an administrator establishes an interactive session and subsequently can enforce an administrator-defined inactivity timeout value after which the inactive session will be terminated. Administrators can also terminate their own interactive sessions as needed.

4.7 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access or HTTPS for web GUI access. The TOE protects communication with network peers, such as a syslog server, using TLS connections. All the underlying algorithms for the specified security protocols are FIPS-certified.

4.8 Intrusion Prevention System

The TOE provides intrusion policies consisting of rules and configurations invoked by the access control policy. The intrusion policies are the last line of defense before the traffic is allowed to its destination. All traffic permitted by the access control policy is inspected by the designated intrusion policy. Using intrusion rules and other preprocessor settings, these policies inspect traffic for security violations and, in inline deployments can block or alter malicious traffic.

If the vendor-provided intrusion policies do not fully address the security needs of the organization, custom policies can improve the performance of the system in the environment and can provide a focused view of the malicious traffic and policy violations occurring on the network. By creating and tuning custom policies the administrators can configure, at a very granular level, how the system processes and inspects the traffic on the network for intrusions.

Using Security Intelligence, the administrators can blacklist—deny traffic to and from—specific IP addresses, URLs, and DNS domain names, before the traffic is subjected to analysis by the access control rules. Optionally, the administrators can use a “monitor-only” setting for Security Intelligence filtering.

5 Assumptions

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

- collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015 with the collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), Version 2.11, 15 June 2017

That information has not been reproduced here and the NDcPP10/IPScEP211 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/IPScEP211 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 Network Devices collaborative Protection Profile and the IPS 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/IPScEP211 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:

- Common Criteria Supplemental User Guide for FirePOWER v6.1, Version 1.0, December 13, 2017

To use the product in the evaluated configuration, the product must be configured as specified in that guide. Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

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 Detailed Test Report (NDcPP10/IPScEP211) for FirePOWER 6.1, Version 0.3, January 3, 2018 (DTR) and as summarized in the publicly available Assurance Activity Report for this evaluation.

8.1 Developer Testing

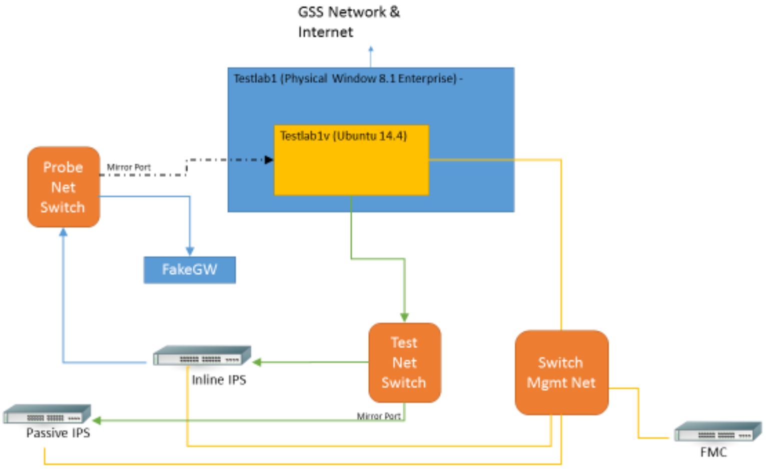
No evidence of developer testing is required in the assurance activities for this product.

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/IPScEP211 including the tests associated with optional requirements. The evaluators used the following tools to support testing.

- SSH Client – Putty version 6.6.1p1
- Big Packet Putty version 6.2
- Wireshark version 2.2.7
- Tcpdump version 4.5.1
- Libpcap version 1.5.3
- Nmap version 6.40
- Nping version 0.6.40
- Hping3 version 3.0.0
- Stunnel version 4.53
- Scapy version 2.2.0

8.3 Test Configuration



9 Evaluated Configuration

The evaluated configuration consists of the following series and models:

FirePOWER Management Center (FMC)

- Cisco FireSIGHT 750 (FS750)
- Cisco FireSIGHT 1500 (FS1500)
- Cisco FireSIGHT 2000 (FS2000)
- Cisco FireSIGHT 3500 (FS3500)
- Cisco FireSIGHT 4000 (FS4000)
- Cisco FireSIGHT Virtual for VMware

FirePOWER IPS/IDS Sensor

Cisco FirePOWER 7000 Series Appliances

- Cisco FirePOWER 7010
- Cisco FirePOWER 7020
- Cisco FirePOWER 7030
- Cisco FirePOWER 7050
- Cisco FirePOWER 7110
- Cisco FirePOWER 7115
- Cisco FirePOWER 7120
- Cisco FirePOWER 7125

Cisco FirePOWER 8000 Series Appliances

- Cisco FirePOWER 8120
- Cisco FirePOWER 8130
- Cisco FirePOWER 8140
- Cisco FirePOWER 8250
- Cisco FirePOWER 8260
- Cisco FirePOWER 8270
- Cisco FirePOWER 8290
- Cisco FirePOWER 8350
- Cisco FirePOWER 8360
- Cisco FirePOWER 8370
- Cisco FirePOWER 8390

Cisco FirePOWER AMP Appliances

- Cisco FirePOWER AMP 7150
- Cisco FirePOWER AMP 8050
- Cisco FirePOWER AMP 8150
- Cisco FirePOWER AMP 8350
- Cisco FirePOWER AMP 8360
- Cisco FirePOWER AMP 8370
- Cisco FirePOWER AMP 8390

Cisco Virtual NGIPS for VMware

All virtual appliances run on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) hardware platforms 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 installed on ISR 4451-X.

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 FirePOWER TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP10/IPScEP211.

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 FirePOWER 6.1 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/IPScEP211 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/IPScEP211 and recorded the results in a proprietary Test Report, and as summarized in the publicly available 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 vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: "firepower", "FMC", "CiscoSSL", "auditd", "syslog-ng", "OpenSSH", "TLS".

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

The AGD states that the PROTECTION license must be purchased and activated to use all the IPS features necessary to meet the IPS Extended Package requirements.

The documentation notes that the following servers are supported in the operational environment.

- NTP Server
- Syslog Server
- SMTP Server
- SNMP Server: SNMP management must not be enabled in the evaluated configuration.
- Authentication Server: use of external authentication server is not allowed in the evaluated configuration unless the channel is securely protected
- Certificate Authority Server
- DNS Server

'Supported' does not mean that the use of those servers has been evaluated, rather it means the vendor asserts that they can be used. Those claims were not verified as part of the evaluation.

If an external audit server is implemented in the operational environment, it is recommended that the administrators configure the system to transmit all the audit events (i.e., audit log and syslog) in real-time over a secure TLS connection to ensure audit records are not lost.
If other servers such as a NTP server are employed, it is suggested that a trusted channel be established between the TOE and those servers.
Other unevaluated functionality includes:

- VPN Gateway
- REST API
- Timeout Exemption Option

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Cisco FirePOWER Version 6.1 Security Target, Version 1.0, January 2, 2018.*

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 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 Network Devices, Version 1.0, 27 February 2015 with the collaborative Protection Profile for Network Devices/collaborative

Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), Version 2.11, 15 June 2017

[5] Cisco FirePOWER Version 6.1 Security Target, Version 1.0, January 2, 2018 (ST)

[6] Assurance Activity Report (NDcPP10/IPScEP211) for FirePOWER 6.1, Version 0.4, January 3, 2018 (AAR)

[7] Detailed Test Report (NDcPP10/IPScEP211) for FirePOWER 6.1, Version 0.3, January 3, 2018 (DTR) <Proprietary Document>

[8] Evaluation Technical Report for Cisco FirePOWER, Version 0.3, January 3, 2018 (ETR) <Proprietary Document>

[9] Common Criteria Supplemental User Guide for FirePOWER v6.1, Version 1.0, December 13, 2017