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 FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv

Report Number: CCEVS-VR-VID10890-2019
Dated: January 30, 2019
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

Dr. Patrick Mallett
The MITRE Corporation
McLean, VA

Jean Petty
Linda Morison
Michelle Carlson
Clare Olin
The MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

Austin Kimbrell
Khai Van
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Architectural Information 3
3.1 TOE Evaluated Platforms 3
3.2 TOE Architecture 4
4 Security Policy 6
4.1 Security audit 6
4.2 Communication 6
4.3 Cryptographic support 6
4.4 Full residual information protection 7
4.5 Identification and authentication 7
4.6 Security management 7
4.7 Protection of the TSF 8
4.8 TOE access 8
4.9 Trusted path/channels 8
4.10 Filtering 8
4.11 Intrusion Prevention System 9
5 Assumptions 9
6 Clarification of Scope 10
7 Documentation 10
8 IT Product Testing 10
8.1 Developer Testing 11
8.2 Evaluation Team Independent Testing 11
9 Evaluated Configuration 11
10 Results of the Evaluation 11
10.1 Evaluation of the Security Target (ASE) 12
10.2 Evaluation of the Development (ADV) 12
10.3 Evaluation of the Guidance Documents (AGD) 12
10.4 Evaluation of the Life Cycle Support Activities (ALC) 13
10.5 Evaluation of the Test Documentation and the Test Activity (ATE) 13
10.6 Vulnerability Assessment Activity (VAN) 13
10.7 Summary of Evaluation Results 14
11 Validator Comments/Recommendations 14
12 Annexes 14
13 Security Target 14
14 Glossary 15
15 Bibliography 15

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv 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 2019. 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 Stateful Traffic Filter Firewalls, version 2.0 + errata 20180314, 14 March 2018 with the Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway, version 2.1, 08 March 2017 and 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 FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv .

The 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 FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv Security Target, Version 1.0, January 15, 2019 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 Product Compliant 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 FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv (Specific models identified in Section 3.1)
Protection Profile	collaborative Protection Profile for Stateful Traffic Filter Firewalls, version 2.0 + errata 20180314, 14 March 2018 with the Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway, version 2.1, 08 March 2017 and 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 FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv Security Target, Version 1.0, January 15, 2019
Evaluation Technical Report	Evaluation Technical Report for Cisco FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv , version 0.3, January 29, 2019
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.

Item	Identifier
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Dr. Patrick Mallet, Jean Petty, Lisa Mitchell, Michelle Carlson, *MITRE Corporation*

3 Architectural Information

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

The Cisco Firepower Threat Defense or FTD is a purpose-built, firewall platform with VPN and IPS capabilities. The Cisco FTD Virtual or FTDv running on UCS platform (TOE) is also a firewall platform with VPN and IPS capabilities. The FMC physical and virtual appliances provide a centralized management console and event database for the FTD and FTDv, and aggregates and correlates intrusion, discovery, and connection data from the FTD and FTDv. In this deployment, the FTD provides VPN, firewall filtering, network analysis, intrusion detection, and access control functionalities.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

TOE Configuration	Hardware Configurations	Software Version
5506-X **5506H-X** **5506W-X** **5508-X** **5516-X**	The Cisco 5500-X Adaptive Security Appliance provides high-performance firewall, VPN, and IPS services and 4-8 Gigabit Ethernet interfaces, and support for up to 300 VPNs.	6.2
5525-X **5545-X** **5555-X**	The Cisco 5500-X Adaptive Security Appliance provides high-performance firewall, VPN, and IPS services and 6-14 Gigabit Ethernet interfaces, and support for up to 5,000 VPNs.	6.2
FS750 **FS1000** **FS2000** **FS2500** **FS4000** **FS 4500**	The Cisco FireSIGHT Series provides centralized management console with up to 4 management interfaces, and up to 10 Gbps speed.	6.2
FMCv **FTDv**	FMCv and FTDv running on ESXi 5.1, 5.5 or 6.0 on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/k9,	6.2

	E160S-M3, and E180D-M2/K9 installed on ISR.	

3.2 TOE Architecture

The TOE consists of one or more FTD physical devices which include the 6.2 software, and the managed by one FMC device. 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. When UI 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. The TOE is able to filter connections to/from these external using its IP traffic filtering, and can encrypt traffic where necessary using TLS, SSH, 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.

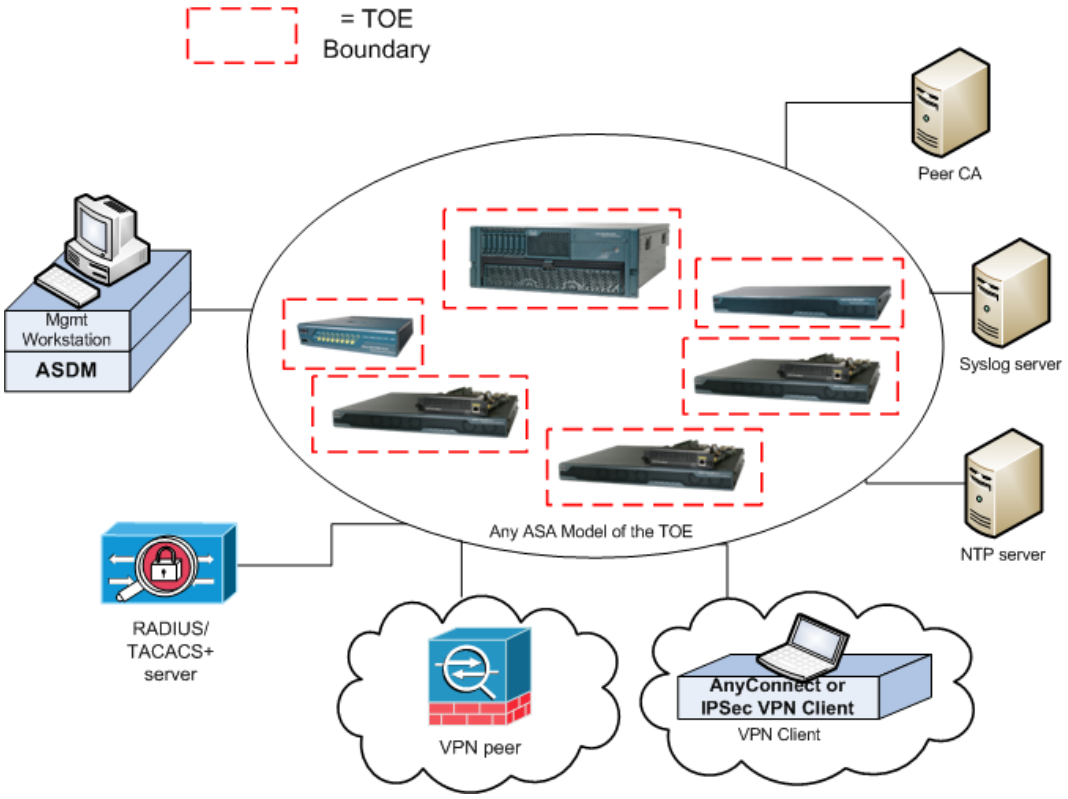

Figure 1: Example TOE Deployment

The 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)
- Peer CA (Operational Environment)
- Syslog server (Operational Environment)

The administrator can configure the FTD either inline or monitor-only (passive) mode. In inline mode, traffic goes through the firewall checks before being forwarded to the Snort engine. When the administrators identify traffic for the Snort engine to inspect, traffic flows through the FTD as follows:

1. Traffic enters the FTD.
2. Incoming VPN traffic is decrypted.
3. Firewall policies are applied.
4. Permitted traffic is sent to the Snort.
5. The Snort applies its security policy to the traffic, and takes appropriate actions.

6. Valid traffic is sent back to the FTD; the Snort might block some traffic according to its security policy, and that traffic is not passed on.
7. Outgoing VPN traffic is encrypted.
8. Traffic exits the FTD.

The TOE can be managed by the CLI and FMC appliance web UI.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security Audit
2. Communication
3. Cryptographic Support
4. Full Residual Information Protection
5. Identification and Authentication
6. Security Management
7. Protection of the TSF
8. TOE Access
9. Trusted Path/Channels
10. Filtering
11. Intrusion Prevention System

4.1 Security audit

The TOE provides extensive 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 Communication

The TOE allows authorized administrators to control which Sensor is managed by the FMC. This is performed through a registration process over TLS. The administrator can also de-register a Sensor if he or she wish to no longer manage it through the FMC.

4.3 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 and TLS/HTTPS. The cryptographic random bit generators (RBGs) are seeded by an entropy noise source.

4.4 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.

4.5 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 threshold has been exceeded.

The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH and HTTPS interfaces. The SSHv2 interface also supports authentication using SSH keys.

4.6 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 or TLS/HTTPS session, or via a local console connection. Management of all security functions can be performed via the FMC/FMCv component of the TOE, while a subset of management functions can be performed on the FTD/FTDv component. 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.

4.7 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, the 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 via FMC. 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.

4.8 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.

4.9 Trusted path/channels

The TOE supports establishing trusted paths between itself and remote administrators using SSHv2 for CLI access and TLS/HTTPS for GUI and web UI access on the FMC. The TOE supports use of TLS and/or IPsec for connections with remote syslog servers. 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.

4.10 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. 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. Port filtering can be configured to restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (service). 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. The File Transfer Protocol is an example of such a protocol, where a data connection is created as needed in response to an explicitly allowed command connection. 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. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. 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.

4.11 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 then 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 Stateful Traffic Filter Firewalls, version 2.0 + errata 20180314, 14 March 2018 with the Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway, version 2.1, 08 March 2017 and 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 FWcPP20E/VPNGWEP21/IPSEP211 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 FWcPP20E/VPNGWEP21/IPSEP211 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 Stateful Traffic Filter Firewalls collaborative Protection Profile, the 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 FWcPP20E/VPNGWEP21/IPSEP211 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:

- FTD (NGFW) v6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv Common Criteria Supplemental User Guide, Version 1.0, January 15, 2019

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 Assurance Activties Report (FWcPP20E/VPNGWEP21/IPSEP211) for Cisco FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv version 0.3, January 29, 2019 (AAR).

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 FWcPP20E/VPNGWEP21/IPSEP211 including the tests associated with optional requirements.

9 Evaluated Configuration

The evaluated configuration consists of the following series and models:

TOE Configuration	Hardware Configurations	Software Version
5506-X **5506H-X** **5506W-X** **5508-X** **5516-X**	The Cisco 5500-X Adaptive Security Appliance provides high-performance firewall, VPN, and IPS services and 4-8 Gigabit Ethernet interfaces, and support for up to 300 VPNs.	6.2
5525-X **5545-X** **5555-X**	The Cisco 5500-X Adaptive Security Appliance provides high-performance firewall, VPN, and IPS services and 6-14 Gigabit Ethernet interfaces, and support for up to 5,000 VPNs.	6.2
FS750 **FS1000** **FS2000** **FS2500** **FS4000** **FS 4500**	The Cisco FireSIGHT Series provides centralized management console with up to 4 management interfaces, and up to 10 Gbps speed.	6.2
FMCv **FTDv**	FMCv and FTDv running on ESXi 5.1, 5.5 or 6.0 on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/k9, E160S-M3, and E180D-M2/K9 installed on ISR.	6.2

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 Cisco FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv TOE to be Part 2 extended, and to meet the SARs contained in the FWcPP20E/VPNGWEP21/IPSEP211.

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 FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv products 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.

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 FWcPP20E/VPNGWEP21/IPSEP211 related to the examination of the information contained in the TSS.

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.

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 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.

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 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.

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 FWcPP20E/VPNGWEP21/IPSEP211 and recorded the results in a Test Report, summarized in the AAR.

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.

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.

1. On the December 21, 2018, the evaluator searched the following sources for vulnerabilities:
    - National Vulnerability Database (https://web.nvd.nist.gov/vuln/search),
    - Vulnerability Notes Database (http://www.kb.cert.org/vuls/),
    - Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities),
    - Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories),
    - Exploit / Vulnerability Search Engin (http://www.exploitsearch.net),
    - SecurITeam Exploit Search (http://www.securiteam.com),
    - Tenable Network Security (http://nessus.org/plugins/index.php?view=search),
    - Offensive Security Exploit Database (https://www.exploit-db.com/)
2. Each site was searched using the following terms:
    a. cisco ftd 6.2
    b. firepower threat defense
    c. ciscossl
    d. router

e. switch
f. TCP
g. IPsec
h. TLS
i. SSH
j. ftd

The public search for vulnerabilities did not uncover any residual vulnerability. 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.

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 validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the. Common Criteria Supplemental User Guide. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the audit server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Cisco FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv Security Target, Version 1.0, January 15, 2019*.

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 Stateful Traffic Filter Firewalls, version 2.0 + errata 20180314, 14 March 2018 with the Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway, version 2.1, 08 March 2017.

[5] Cisco FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv Security Target, Version 1.0, January 15, 2019 (ST).

[6] Assurance Activity Report (FWcPP20E/VPNGWEP21/IPSEP211) for Cisco FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv , Version 0.3, January 29, 2019 (AAR).

[7] Detailed Test Report (FWcPP20E/VPNGWEP21/IPSEP211) for Cisco FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv, Version 0.3, January 29, 2019 (DTR).

[8] Evaluation Technical Report for Cisco FTD (NGFW) 6.2 on ASA 5500-X and FTDv with FireSIGHT (FMC) and FMCv , Version 0.3, January 29, 2019 (ETR)