National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

General Dynamics C4 Systems

Fortress Mesh Point ES210

Report Number: CCEVS-VR-VID10571-2014
Dated: December 4, 2014
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 Panel

Patrick Mallett

The MITRE Corporation, McLean, VA

Daniel Faigin

The Aerospace Corporation, El Segundo, CA

Common Criteria Testing Laboratory

Scott Cutler

Ryan Day

Kenji Yoshino

InfoGard Laboratories, Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the Fortress Mesh Point ES210.

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

The TOE, the Fortress Mesh Point ES210, is a device that manages inbound and outbound traffic on an 802.11a/b/g/n wireless network. It is used to provide secure wireless communications to environmentally challenging situations, including outdoor locations. The TOE protects data exchanged with wireless client devices using IEEE 802.11i wireless security protocol (WPA2), and protects data exchanged with wired devices using IPsec, TLS, HTTPS, and SSH.

2 Identification of the TOE

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 organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Fortress Mesh Point ES210 Hardware Versions: ES210-3: 710-00020-01 ES210-4: 710-00033-01 Software Version: 5.4.3.1608
Protection Profile	Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 01 December 2011
Security Target	FORTRESS Mesh Point ES210 Security Target, Version 2.0, December 5, 2014
Dates of Evaluation	6/3/12 – 11/11/14
Conformance Result	Pass
Common Criteria Version	v3.1 Revision 3
Common Evaluation Methodology (CEM) Version	v3.1 Revision 3
Evaluation Technical Report (ETR)	Evaluation Technical Report, 14-2686-R-0028 Version 1.3, December 2, 2014
Assurance Activities Report (AAR)	Assurance Activity Report, 14-2686-R-0029 Version 1.5, December 5, 2014
Sponsor/Developer	General Dynamics C4 Systems
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Scott Cutler, Ryan Day, Kenji Yoshino
CCEVS Validators	Patrick Mallett, Daniel Faigin

Table 1: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before June 3, 2014.

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

Audit
Cryptography
User Data Protection
Identification and Authentication
Security Management
Protection of the TSF
TOE Access
Trusted Path/Channels

4.1 Audit

The TOE has the ability to audit events based on a variety of specified criteria. To protect the TSF from audit log overflow, the TOE uploads audit data to an external syslog server through an IPSEC tunnel. The audit record includes: the date and time of the event, the user who triggered the event (if event was user based and user is known), and event specific information. The types of events that are audited are seen in the ST. The TOE also protects all locally stored audit data from un-authorized modification and deletion. If the syslog server is unavailable, the TOE stops sending packets to the syslog server, and adds a “Communication error” message to the local log.

4.2 Cryptography

The TOE provides cryptographic functions to protect information, including mechanisms to encrypt, decrypt, hash, digitally sign, and perform cryptographic key agreement. The evaluated configuration uses a subset of the FIPS 140-2 compliant cryptographic implementations (listed in Section 12 of the ST) for all cryptographic purposes. The cryptographic algorithms used are those specified by the SFR’s. The associated FIPS compliance certificates, and list of the protocols that use the cryptography features, are listed below:

- WPA2 (802.11i)
- WPA2 (EAP-TLS)
- IPsec
- SSHv2
- HTTPS/TLS

Algorithm	Cert #	Implementation	Firmware Version	Functionality	Operational Environment[1]	Modes
AES	1519	Fortress Cryptographic Implementation	2.0	IPsec, WPA2	RMI Alchemy MIPS Processor, Broadcom XLS Processor	ECB (e/d; 128 , 192 , 256) CBC (e/d; 128 , 192 , 256);
	1520	Fortress Cryptographic Implementation - FPGA	2.0	IPsec, WPA2	Xilinx Spartan FPGA	CBC (e/d; 128, 192, 256) CCM (KS: 128)
	1512	Fortress Cryptographic Implementation - SSL	2.0	IPsec, WPA2, TLS, SSH	RMI Alchemy MIPS Processor, Broadcom XLS Processor	ECB (e/d; 128, 192 , 256) CBC (e/d; 128, 192, 256) CFB8 (e/d; 128, 192, 256) CFB128 (e/d; 128, 192, 256) OFB (e/d; 128, 192, 256)
SHS	1357	Fortress Cryptographic Implementation	2.0	WPA2 IPsec	RMI Alchemy MIPS Processor, Broadcom XLS Processor	SHA-1 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)
	1358	Fortress Cryptographic Implementation - FPGA	2.0	WPA2 IPsec	Xilinx Spartan FPGA	SHA-1 (BYTE-only) SHA-384 (BYTE-only)

[1] "RMI Alchemy MIPS Processor" was previously "AMD Alchemy MIPS Processor" due to acquisition.

Algorithm	Cert #	Implementation	Firmware Version	Functionality	Operational Environment[1]	Modes
	1355	Fortress Cryptographic Implementation - SSL	2.0	TLS SSH WPA2	RMI Alchemy MIPS Processor, Broadcom XLS Processor	SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)
HMAC	889	Fortress Cryptographic Implementation	2.0	WPA2 IPsec	RMI Alchemy MIPS Processor, Broadcom XLS Processor	HMAC-SHA1 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512
	890	Fortress Cryptographic Implementation - FPGA	2.0	WPA2 IPsec	Xilinx Spartan FPGA	HMAC-SHA1 HMAC-SHA384
	887	Fortress Cryptographic Implementation - SSL	2.0	TLS SSH WPA2	RMI Alchemy MIPS Processor, Broadcom XLS Processor	HMAC-SHA1 HMAC-SHA224 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512
RNG	822	Fortress Cryptographic Implementation - FPGA	2.0	WPA2 IPsec	Xilinx Spartan FPGA	ANSI X9.31 [TDES-2Key]
RSA	740	Fortress Cryptographic Implementation - SSL	2.0	TLS SSH IPsec	RMI Alchemy MIPS Processor, Broadcom XLS Processor	FIPS186-2: ALG[RSASSA-PKCS1_V1_5] SIG(ver): 2048, SHS: SHA-1 SIG(gen): 2048, SHS:SHA-1
DRBG 800-90	65	Fortress Cryptographic Implementation - SSL	2.0	TLS SSH WPA2	RMI Alchemy MIPS Processor, Broadcom XLS Processor	HMAC_Based DBRG: SHA-1, SHA-256, SHA-384, SHA-512

Algorithm	Cert #	Implementation	Firmware Version	Functionality	Operational Environment[1]	Modes
	66	Fortress Cryptographic Implementation	2.0	IPsec	RMI Alchemy MIPS Processor, Broadcom XLS Processor	HMAC_Based DBRG: SHA-1, SHA-256, SHA-384, SHA-512
KAS	10	Fortress KAS Implementation	1.0	IPsec	RMI Alchemy MIPS Processor, Broadcom XLS Processor	FFC: SHA-256 ECC: P-256 SHA-256 HMAC ED: P-384 SHA-384 HMAC

Table 2: CAVP Certificates

4.3 User Data Protection

The TOE protects user data, (i.e., only that data exchanged with wireless client devices), using the IEEE 801.11i standard wireless security protocol, mediates the flow of information passing to and from the WAN port, and ensures that resources used to pass network packets through the TOE do not contain any residual information.

4.4 Identification and Authentication

The TOE requires the system administrators be authenticated before access to the TOE is granted; administrators may login to the TOE via a local RJ45 using a serial RS-232 connection, and remotely via SSH, HTTPS, or X/509 for TLS. Administrators may connect to the TOE remotely via the LAN, WAN, or 802.11a/b/g/n interfaces.

The TOE displays a configurable access banner and enforces administrator password for administrative authentication. An external RADIUS server can be configured for authentication through an IPsec tunnel. Authentication can take place, either by user name and password (and hexadecimal device ID if applicable) and 802.1x EAPOL. For IPsec, the TOE also supports X.509 certificates. EAP-TLS is used for WPA2 wireless authentication via x.509 certificates.

4.5 Security Management

The management of the security relevant parameters of the TOE is performed by the authorized administrator; the TOE provides the following management interfaces:

- Command Line Interface (CLI) via
  - local RJ45 or serial connection,
  - Remote SSH interface via the LAN, WAN ports, and 802.11 wireless interface
- Remote HTTPS Web UI via the LAN, WAN ports, and 802.11 wireless

4.6 Protection of the TSF

The TOE identification and authentication security functions allow only authenticated administrative users direct access to the TOE. If a wireless user does not authenticate as an administrative user then that user is a wireless client and can only pass traffic through the TOE and cannot execute commands on the TOE.

Administrative users are allowed to login via the CLI and Web UI to access all management functions. The management interfaces do not allow administrative users access to the underlying operating system and there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE. Any access to a management interface (CLI or GUI) is protected by a secure channel except via RS-232; as this is considered local administration.

The TOE has the capability to obtain reliable time from a remote Network Time Protocol (NTP) Server to provide reliable time stamps for audit services. Additionally, the system administrator can manually set the time (maintained locally in the hardware Real Time Clock (RTC)) on the TOE using the Web UI or CLI management interfaces.

The TOE runs a set of self-tests on power-on and on demand to verify the correct operation of the TOE's underlying hardware, TOE software and cryptographic modules. Additional cryptographic tests are performed during normal operation. The security of network data is maintained by ensuring no residual information is included in network packets.

4.7 TOE Access

The TOE displays the access banner before establishing an administrative session. This is displayed prior to an administrator authenticating to the TOE. The TOE terminates an interactive session after an Authorized Administrator-configurable time interval of session inactivity. A wireless client session is defined as being allowed access to a particular port on the application layer. The TOE is able to deny establishment of a wireless client session based mac address and IP address.

4.8 Trusted Path/Channels

The TOE uses 802.11-2007 and IPsec to provide a trusted communication channel between itself and any authorized IT entities that are logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data. In addition to IPsec, EAP-TLS is used for RADIUS.

The TSF shall initiate communication via the trusted channel for RADIUS, NTP and Syslog. The TOE uses SSH and TLS/HTTPS to provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
A.NO_TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.

5.2 Operational Environment Requirements

This table identifies components that must be present in the Operational Environment to support the operation of the TOE.

Component	Description
Syslog server	Compatible with RFC 5424, Supporting IPsec
RADIUS server	Compatible with RFC 2865, Supporting IPsec
NTP server	V4 conformant to RFC 5905, Supporting IPsec
GUI access	Firefox v3.6 to 14, IE version 7-9
CLI access	SSH V2 client

Table 3: Operational Environment Components

5.3 Limitation of Scope

The scope of the evaluation is limited to the functionality specified by the Wireless Local Area Network (WLAN) Access Device for Common Criteria Protection Profile. Although the TOE includes other cryptographic and network protocol functionality, the evaluation only includes the cryptographic algorithms and protocols specified by the Protection Profile (TLS, SSH, HTTPS, WPA2, IPsec). The TOE guidance specifies the settings required to enable the cryptographic protections evaluated by the CCTL, and also specifies any settings that are explicitly disallowed by the Protection Profile requirements.

6 Architectural Information

The TOE is classified as Wireless Local Area Network (WLAN) Access Device for Common Criteria purposes. The TOE is made up of *hardware and software* components.

The TOE is delivered in a form factor that is rugged, weatherized, and easy to set-up. The TOE functions as both a wireless access point and bridge, with one powerful radio.

6.1 Architecture Overview

The TOE consists of two models, the ES210-3 and ES210-4. The hardware versions for each model respectively are 710-00020-01 and 710-00033-01. All models use the same software image: 5.4.3.1608. The chipsets between models are the same, and only differ by the radios included in the device.

6.1.1 TOE Hardware

The physical boundaries of the ES210 are at all of the connectors of the TOE module:

- RJ45 10/100BT Ethernet Port (2)
    - Provides a port for the user to access the network as well as allows access to the management functionality with administrative user authentication. The only difference between the two ports is that the port labeled (WAN) is encrypted by default, the other is not.
- 3 Pin Con-X Serial Connector (3 pin mil-spec round connector)
    - Local CLI management interface.
- 2 Pin Con-X Power Connector (2 pin mil-spec round connector)
    - Provides power to the ES210
- RP-TNC Antenna Connector (1)
    - ES210-3
        - Radio 1: 250mW 802.11a/b/g/n 2.4GHz, 4.9GHz, or 5GHz
    - ES210-4
        - Radio 1: 600mW 802.11a/n 4.4GHz
- SMA Connector
    - GPS antenna

Indicators are used to allow the operator to have a quick indication of the state of the ES210:

- Power
    - Indicates the power status of the TOE
- Battery
    - Indicates the charge state of the battery
- Ethernet1/Ethernet 2 – Link/Activity
    - Indicates the status and activity of the Ethernet port
- Radio activity
    - Indicates activity on the radio
- Crypto
    - Not used

The ES210 also has the following physical button controls:

- Power On/Off
    - Allows the device to be powered.
- Blackout Mode

    - Turns off all LED indicators.
- RF Kill
    - Turns all radio transmissions off.
- Zeroize
    - Restores factory defaults.

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Fortress Mesh Point ES210. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is shown with a hashed background.

The TOE hardware and software versions are verified by the user upon delivery. The guidance documents are provided through the vendor's support website and personnel and apply to the CC Evaluated configuration:

7.1 Guidance Documentation

Document	Revision	Date
Fortress Common Criteria Operational Guidance	1.18	December 2, 2014
ES210 Tactical Mesh Point Hardware Guide	Rev. 3	N/A
Fortress Mesh Point Software Auto Configuration Guide	009-00037-00v5.4.3r1	N/A
Fortress Mesh Point and Network Encryptor Software CLI Guide	009-00036–00v5.4.3r2	N/A
Fortress Mesh Point and Network Encryptor Software GUI Guide	009-00035-00v5.4.3r1	N/A
Fortress Common Criteria Supplemental Operational Guidance for Logging Requirements.	1.4	April 11, 2013
Release Notes Mesh Point version 5.4.3	R2	N/A
MIB Files	N/A	N/A
Radius Files	N/A	N/A

7.2 Security Target

Document	Revision	Date
FORTRESS Mesh Point ES210 Security Target	2.0	December 5, 2014

8 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

8.1 Evaluation Team Independent Testing

The evaluation team performed all testing activities specified in the Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 01 December 2011. The test environment consisted of the following equipment:

The following equipment was used to perform independent testing of the TOE:

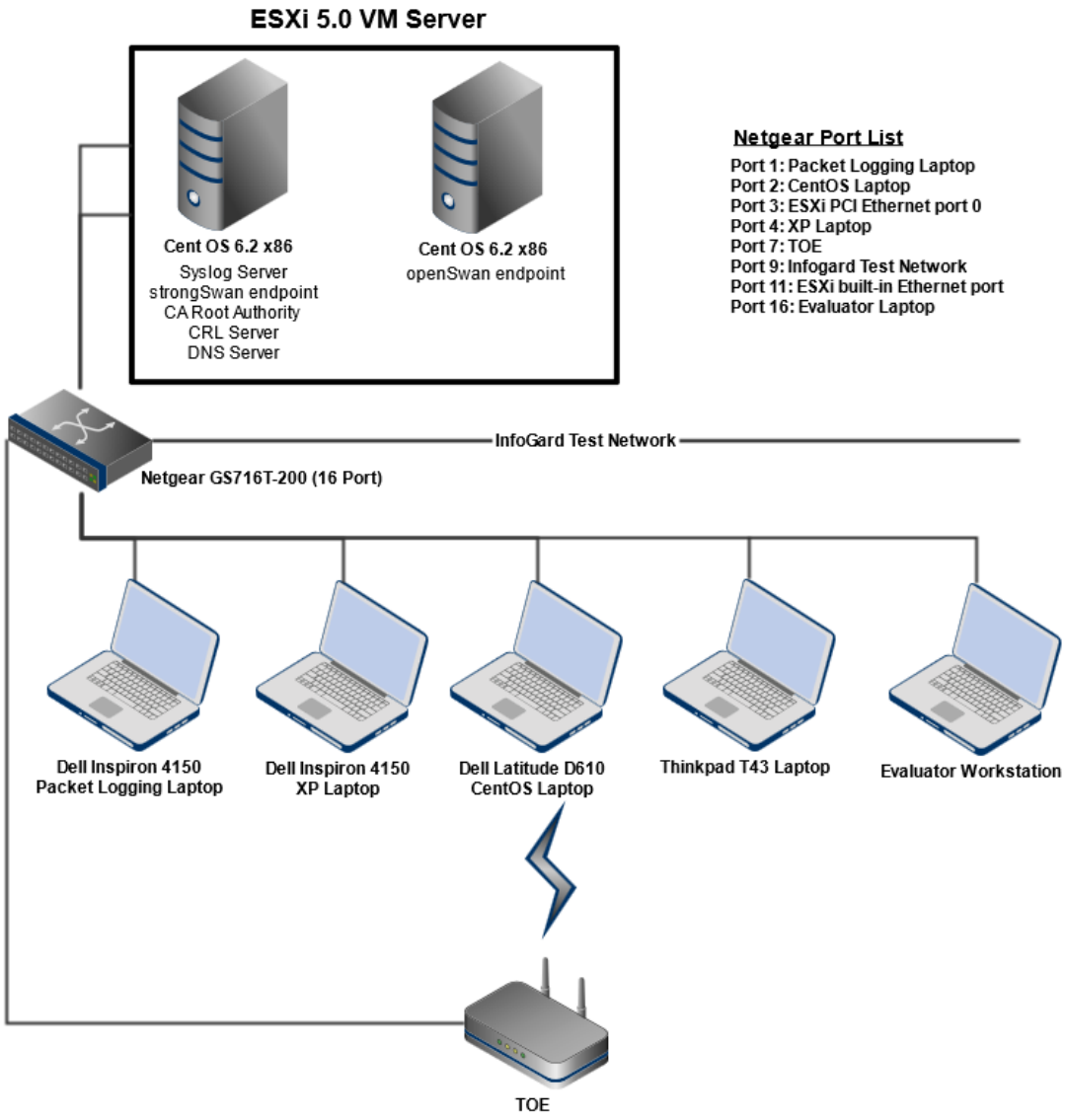
Quantity	Description	Purpose
1	Netgear GS716T-200 ProSafe 16-port Smart Switch	Ethernet switch
1	Dell Inspiron 4150 Laptop (1 Ethernet port)	Packet Logger
1	Dell Inspiron 4150 Laptop (1 Ethernet port)	Windows XP Test Device
1	Dell Latitude D610 Laptop (1 Ethernet port)	CentOS Test Device
1	Dell Poweredge 840 (1TB HD, 8 GB RAM, 1 built-in Ethernet)	ESXi 5.0 VM Host
1	InfoGard-issued evaluator laptop (Windows, 1 Ethernet port)	Configuration, test management
1	Broadcom 4-port PCI gigabit Ethernet Adapter	ESXi 5.0 Ethernet Connectivity
1	Dlink Airplus-G PCMCIA 802.11b\g Adapter	Wireless Network Interface
8	10ft. Cat5e Ethernet Cables	Ethernet connectivity
1	Fortress ES210-3 Mesh Point	TOE

The following versions of software were used:

Software	Version
Firefox	10.0.5
freeRADIUS	2.1.10
rsyslogd	5.8.12

BIND	9.8.2-0.17
NTP	4.2.4p8-2
omping	0.0.4-1.el6
StrongSwan	5.0.0

The final test environment diagram is included below:



Using the above test environment as a baseline, the evaluation team created 51 test procedures to perform testing. Each test case corresponded to one or more assurance activities and associated SFRs from the [PP]. Each test was independent of the other (with two noted

exceptions), and any changes to the test environment baseline were reset after each test case. Each test procedure included the following information: Description/Goal, Assurance Activity, Setup, TOE Model, Test Steps, Expected Results, Actual Results, Date Tested, Evaluator Name, and Overall Verdict. An overall table of the 51 test procedures is included in the table below:

Assurance Activities	Description
FAU_GEN.1 (Test 1)	Audit of Administrator Actions
FAU_GEN.1 (Test 2)	Audit of Assurance Activities
FAU_SEL.1	Audit Event Selection
FAU_STG_EXT.1	External Audit Trail Storage
FAU_STG_EXT.3	Action in Case of Loss of Audit Server Connectivity
FCS_CKM.1(2)	Asymmetric Key Generation
FCS_CKM.2(1)	802.11 Pairwise Master Key Protection
FCS_CKM.2(2)	802.11 Group Temporal Key
FCS_COP.1(1)	Data Encryption/Decryption
FCS_COP.1(2)	Cryptographic Signature
FCS_COP.1(3)	Hashing
FCS_COP.1(4)	Keyed Hash Message Authentication
FCS_COP.1(5)	WPA2 Data Encryption\Decryption
FCS_IPSEC_EXT.1	NAT Traversal
FCS_IPSEC_EXT.1.2	ESP Confidentiality and Integrity Security Mode
FCS_IPSEC_EXT.1.3	IKEv1 Phase 1 Aggressive\Main Mode
FCS_IPSEC_EXT.1.4 (Test 1-2)	IKEv1 8 and 24 Hour Timeout
FCS_IPSEC_EXT.1.4 (Test 3)	SA Packet Number Limit
FCS_IPSEC_EXT.1.4 (Test 4)	IKEv2 SA Custom Time Timeout
FCS_IPSEC_EXT.1.7, FCS_IPSEC_EXT.1.10 (Test 1-2)	Algorithm Support
FCS_IPSEC_EXT.1.8 (PSK Test 1), FIA_PSK_EXT.1	PSK Authentication
FCS_IPSEC_EXT.1.8 (X.509 Test 1-2)	X.509 Authentication
FCS_IPSEC_EXT.1.8 (X.509 Test 3-4), FIA_X509_EXT.1 (Test 1)	Invalid Certificates

FCS_RGB_EXT.1	Random Bit Generation
FIA_AFL.1, FCS_SSH_EXT.1.3 (Test 2)	Authentication Failure Limit
FIA_PMG_EXT.1 (Test 1, 3), FIA_UAU.6	Password Management
FIA_PMG_EXT.1 (Test 2)	Password Management
FIA_UAU.7, FIA_UIA_EXT.1 (Test 1, 3)	Local Identification and Administration
FIA_UIA_EXT.1 (Test 2), FTP_TRP.1 (Test 2)	Available Services
FIA_8021X_EXT.1	RADIUS \ EAP-TLS Authentication
FIA_PSK_EXT.1	Pre-Shared Key Support
FIA_X509_EXT.1	X.509 Certificate Support
FMT_SMR.1	Disallow Wireless Clients
FPT_TST_EXT.1	TSF Testing
FPT_TUD_EXT.1	Software Updates
FRU_RSA.1	Resource Management
FTA_SSL_EXT.1, FTA_SSL.4 (Test 1)	Local Session Timeout and Termination
FTA_SSL.3, FTA_SSL.4 (Test 2), FCS_SSH_EXT.1.4 (Test 2), FTP_TRP.1 (Test 1)	Remote Session Timeout , Termination, and Connection
FTA_TAB.1	Access Banner
FTA_TSE.1	Client Session Filtering
FTP_ITC.1 (Test 1-3)	Encrypted Communications
FTP_ITC.1 (Test 4)	Channel Data Modification
FTP_ITC.1 (Test 5)	Physical Interruption
FTP_TRP.1 (Test 3)	Encrypted Communications
FTP_TRP.1 (Test 4)	Channel Data Modification
FCS_SSH_EXT.1.3 (Test 1)	Authentication Timeout
FCS_SSH_EXT.1.4 (Test 1)	Public Key Authentication
FCS_SSH_EXT.1.5	Large Packets
FCS_SSH_EXT.1.6	Algorithm Support
FCS_SSH_EXT.1.9	Diffie-Hellman Support
FCS_TLS_EXT.1, FTP_TRP.1 (Test 1)	Ciphersuite Support

The TOE passed all required test activities.

8.2 Vulnerability Analysis

On June 11, 2014 the evaluation team searched http://www.cvedetails.com for known vulnerabilities in:

- Fortress
- ES210
- ES520
- ES820
- ES2440.

We were unable to find any applicable vulnerabilities.

The evaluation team determined that suitable vulnerabilities would have Low CVSSv2 Access Complexity, because a Medium Access complexity as defined by http://www.first.org/cvss/cvss-guide.html#i2.1.2 requires additional access, social engineering, and/or a non-default configuration.

The evaluation team researched web articles to determine vulnerabilities for similar devices, and ruled out the suitability or possibility for any vulnerabilities affecting the TOE in its evaluated configuration. The evaluation team performed a general web vulnerability scan and found six vulnerabilities, however none were suitable or applicable to the TOE in its evaluated configuration.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.

InfoGard has determined that the TOE meets the security criteria in the Security Target, which specifies an assurance requirements specified in Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 01 December 2011. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in December 2014.

10 Validator Comments/Recommendations

The validators note that this validation was conducted in parallel with the validations of the TOE's siblings. Listed below are the Fortress Mesh Point wireless devices that were evaluated in

each evaluation:

- VID10571: includes models ES210-3 and ES210-4
- VID10572: includes models ES520-35, ES520-34, ES820-35, and ES820-34
- VID10573: includes models ES2440-3555, ES2440-3444, ES2440-35, and ES2440-34.

11 Security Target

FORTRESS Mesh Point ES210 Security Target, Version 2.0, December 5, 2014

12 Terms

12.1 Acronyms

CC	Common Criteria
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
FIPS	Federal Information Processing Standards Publication 140-2
HTTP	Hyper Text Transfer Protocol
IEEE 801.11i	Institute of Electrical and Electronics Engineers 802.11i Wireless Standard
IPsec	Internet Protocol Security
IT	Information Technology
NIST	National Institute of Standards and Technology
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
SF	Security Functions
SFR	Security Functional Requirements
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
WLAN	Wireless Local Area Network

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1 Revision 3, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.

[5] Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 01 December 2011