National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

[Apriva ISS, LLC.]

[Apriva MESA VPN server, v1.0, build 21.16]

Report Number: CCEVS-VR-10602-2015
Dated: **August 7, 2015**
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

Daniel Faigin

The Aerospace Corporation, El Segundo, CA

Meredith M Hennan

The Aerospace Corporation, Houston, TX

Common Criteria Testing Laboratory

Scott Cutler, Ryan Day

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 Apriva MESA VPN server, v1.0, build 21.16.

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 Apriva MESA VPN server is an IPsec VPN gateway designed to provide mobile devices with a secure connection to a protected network.

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

Component	Description
Syslog Server	Syslog Server supporting Syslog over TLSv1.2 with ciphersuites: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA Conforming to: • RFC 5424 (Syslog) • RFC 5425 (Syslog over TLS) • RFC 5246 (TLSv1.2)

VPN Clients	VPN Clients supporting:
	• IPsec/IKEv2 (RFC 5996)
	  ○ Authentication with X.509 using:
	  ▪ RSA
	  ▪ ECDSA
	  ○ Symmetric ciphers:
	  ▪ AES-CBC-128
	  ▪ AES-CBC-256
	  ○ Integrity Algorithms:
	  ▪ HMAC-SHA-256
	  ▪ HMAC-SHA-384
	  ▪ HMAC-SHA-512
	  ○ Key Agreement
	  ▪ Diffie-Hellman Group 14
	  ▪ Diffie-Hellman Group 19
	  ▪ Diffie-Hellman Group 20
	  ▪ Diffie-Hellman Group 24
	• IPsec/ESP (RFCs 4301 & 4303)
	  ○ Tunnel Mode
	  ○ Symmetric ciphers:
	  ▪ AES-GCM-128
	  ▪ AES-GCM-256
	  ○ Integrity:
	  ▪ N/A (provided by AES-GCM)

NTP Server	NTP Server supporting NTPv4 (RFC 5905)
Local Console	Local Console supporting RS-232 connection

SSH Client	SSH Client (Remote Console) supporting:
	• SSHv2 (RFCs 4250, 4251, 4252, & 4253)
	• Symmetric Ciphers:
	  ○ AES-CBC-128
	  ○ AES-CBC-256
	• Integrity Algorithm:
	  ○ HMAC-SHA-1
	• Key Agreement:
	  ○ Diffie-Hellman Group 14 SHA-1
	• Server Authentication:
	  ○ SSH_RSA
	• Client Authentication:
	  ○ SSH_RSA
	  ○ Password

Table 1: Operational Environment Components

2 Identification of the TOE

Table 2 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	Apriva MESA VPN server, v1.0, build 21.16
Protection Profile	• Protection Profile for Network Device Protection Profile, Version 1.1, June 8, 2012 • Security Requirements for Network Devices Errata #3, November 3, 2014 • Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, April 12, 2013 • TD0013: AVA_VAN.1 in VPN GW EP, September 15, 2014 • TD0004: FCS_TLS_EXT Man-in-the-Middle Tests, May 28, 2014
Security Target	Apriva MESA VPN Server Security Target, Version 0.10, July 15, 2015
Dates of Evaluation	March 2, 2015 – July 15, 2015
Conformance Result	Pass
Common Criteria Version	v3.1 Revision 3
Common Evaluation Methodology (CEM) Version	v3.1 Revision 3
Evaluation Technical Report (ETR)	Common Criteria Evaluation Technical Report, DOC ID: 15-3117-R-0011 V1.1, July 20, 2015
Assurance Activities Report (AAR)	Common Criteria Assurance Activity Report, DOC ID: 15-3117-R-0012 V1.1, July 20, 2015
Sponsor/Developer	Apriva ISS, LLC.

Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc. 709 Fiero Ln, Ste. 25 San Luis Obispo, CA 93401
CCTL Evaluators	Scott Cutler, Ryan Day
CCEVS Validators	Daniel Faigin, Meredith M Hennan

Table 2: 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 March 2, 2015.

During the course of the evaluation, interpretations were made by both TD and the TRRT. Please refer to Section 7.3 - Validator and NIAP Guidance for a complete list of evidence containing these interpretations.

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
- Packet Filtering
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

The following features were not evaluated and the impact of their use has not been assessed:

- Local redundancy
- NTP server
- DNS client
- SNMP (Simple Network Management Protocol)
- OSPF (Open Shortest Path First)
- DMCC support (DoD Mobility Classified Capability)
- Single-user mode (allows the user to recover the device)

Additional details and warnings are provided in guidance that inform the user of any commands or options that may violate the CC evaluated configuration.

4.1 Audit

The TOE generates audit records for security relevant events. The TOE maintains a local audit log as well as sending the audit records to a remote Syslog server. Audit records sent to the remote server are protected by a TLSv1.2 connection. Each audit record includes identity (username, IP address, or process), date and time of the event, type of event, and the outcome of the event. The TOE prevents modification to the local audit log.

4.2 Cryptographic Operations

The TOE implements CAVP validated cryptographic algorithms for random bit generation, encryption/decryption, authentication, and integrity protection/verification. These algorithms are used to provide security for the SSH, TLS, and IPsec (IKEv2 and ESP) protocols.

- Red Hat Enterprise Linux Kernel Crypto Module
  - AES-GCM (Cert #2983)
- OpenSSL FIPS Object Module v2.0.5 (FIPS 140-2 Cert #1747)
  - AES (Cert #2484)
  - SHA-1, 224, 256, 384, 512 (Cert #1526)
  - HMAC SHA-1, 224, 256, 384, 512 (Cert #1526)
  - CTR_DRBG (AES-256) (Cert #342)
  - RSA (Cert #1273)
  - ECDSA (Cert #413)
- QuickSec
  - CTR_DRBG (AES-256) (Cert #570)

The TOE zeroizes all plaintext secret and private cryptographic keys and CSPs once they are no longer required.

4.3 User Data Protection

The TOE ensures that previous content of network packets is not reused in subsequent network packets. The TOE zeroizes IPsec buffers when the packet has been transmitted. The TOE ensures that all other network buffers are zeroized upon allocation of the buffer.

4.4 Identification and Authentication

The TOE authenticates administrative users using a username/password combination or a username/SSH_RSA key combination. The TSF does not allow access to any administrative functions prior to successful authentication. The TOE has the capability to lock a remote user's account if that user exceeds the configured number of failed authentication attempts.

4.5 Security Management

The TOE implements a limited command line interface (CLI) to allow authorized administrators to configure the TOE. This interface restricts the administrator to executing commands required to configure and administer the TOE.

4.6 Packet Filtering

The TOE filters packets received on the physical interfaces and virtual interfaces (IPsec tunnels). The TOE reads each packet's header and can be configured to allow or deny the packet based on IPv4 source address, IPv4 destination address, Transport Layer Protocol (if specified in an IPv4 header), TCP or UDP source port, and TCP or UDP destination port.

4.7 Protection of the TSF

The TOE protects itself through a number of features. The CLI does not provide commands for the administrator to display secret and private keys. The TOE ensures timestamps and timeouts are accurate by maintaining a real-time clock for measuring time as well as polling an NTP server to mitigate drift.

The TOE implements self-tests to verify its correct operation prior to offering protected services (VPN functionality). If the initial self-tests fail or the ongoing health tests fail, the TOE shuts down the VPN functionality and blocks all traffic to or from the network interfaces that were running VPN tunnels.

The TOE automatically verifies the authenticity and integrity of updates by requiring the updates to be digitally signed. TOE verifies that every update is signed by Apriva prior to installing the update.

4.8 TOE Access

The TOE can be configured to display a warning and consent banner when an administrator attempts to establish an interactive session. The TOE also enforces a configurable inactivity timeout for remote administrative and IPsec sessions.

The TOE can be configured to deny establishment of a VPN client session based on the time, day, and/or remote client's IP address.

4.9 Trusted Path/Channels

The TOE uses IPsec or TLS to provide a trusted communication channel between itself and all authorized IT entities. The trusted channels utilize X.509 certificates to perform mutual authentication. The TOE initiates the TLS trusted channel with the Syslog server while the TOE allows the remote VPN clients to initiate the IPsec trusted channel.

The TOE uses SSH to provide a trusted path between itself and remote administrative users.

5 TOE Security Environment

5.1 Secure Usage Assumptions

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

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.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T.NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network
T.NETWORK_MISUSE	Access to services made available by a protected network might be used counter to Operational Environment policies.
T.REPLAY_ATTACK	If malicious or external IT entities are able to gain access to the network, they may have the ability to capture information traversing

	throughout the network and send them on to the intended receiver.
T.DATA_INTEGRITY	A malicious party attempts to change the data being sent – resulting in loss of integrity.
T.UNAUTHORIZED_CONNECTION	While a VPN client may have the necessary credentials (e.g., certificate, pre-shared key) to connect to a VPN gateway, there may be instances where the remote client, or the machine the client is operating on, has been compromised and attempts to make unauthorized connections.
T.HIJACKED_SESSION	There may be an instance where a remote client's session is hijacked due to session activity. This could be accomplished because a user has walked away from the machine that was used to establish the session.
T.UNPROTECTED_TRAFFIC	A remote machine's network traffic may be exposed to a hostile network. A user may be required to use a hostile (or unknown) network to send network traffic without being able to route the traffic appropriately.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

6 Architectural Information

The TOE is classified as Virtual Private Network for Common Criteria purposes. The TOE is made up of hardware and software components.

6.1 Architecture Overview

The TOE consists of a Dell™ PowerEdge™ R720 running Apriva MESA VPN server v1.0, build 21.16.

6.1.1 TOE Hardware

- Dell™ PowerEdge™ R720
  - CPU: Intel® Xeon® processor E5-2600 series
  - RAM: 16GB
  - NICs: Qty 4, 1Gb/s
  - Disks: Qty 4, 300GB SAS Hot Pluggable, RAID-1
  - Power Supply: Qty 2, Hot Pluggable
  - CD/DVD: Qty 1, SATA
  - Enhanced Hardware Entropy Generation: QUANTIS PCIe card

6.1.2 TOE Software

- Apriva MESA VPN server v1.0, build 21.16
  - Red Hat Enterprise Linux 6.4
  - QuickSec

- OpenSSL FIPS 2.0.5
- Syslog-ng Premium Edition 5

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 Apriva MESA VPN server. 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 is delivered using an insured and tracked commercial courier service. The guidance documents are provided on a CD and apply to the CC Evaluated configuration:

7.1 Guidance Documentation

Document	Revision	Date
Apriva MESA VPN, NIAP Guidance	**Version 1.0**	**July 16, 2015**
APRIVA MESA VPN VERSION 1.0 VPN 21 16 Release_Notes	**N/A**	**N/A**

7.2 Security Target

Document	Revision	Date
Apriva MESA VPN Security Target	0.10	July 15, 2015
Entropy Documentation and Assessment	N/A	January 13, 2015
Analysis of the Linux Random Number Generator	N/A	March 6, 2006
RANDOMNESS TEST REPORT	2.0	April 2010
TRUE RANDOM NUMBER GENERATOR BASED ON QUANTUM PHYSICS	N/A	N/A
ID Quantique White Paper RANDOM NUMBER GENERATION USING QUANTUM PHYSICS	3.0	April 2010

7.3 Validator and NIAP Guidance

Document	Date
TD0004: FCS_TLS_EXT Man-in-the-Middle Tests	May 28, 2014

TD0013: AVA_VAN.1 in VPN GW EP	September 15, 2014
NDPP VPN EP Questions_Response.docx	January 2014
Re NDPP FIPS question.msg	October 2014
VPN TRRT Questions.docx, Re trrt-vpngateway VPN GW EP Questions.msg	December 2014
TRRT_Questions_VID10602_scutler_InfoGard_v2.docx, Re trrt-vpngateway VID 10602 Question 1.msg	January 2015
May 2015.zip	May 2015
vid10602-0001-MR-Pre-Kickoff-Comments-dpfaigin.docx	December 2014 - January 2015

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 Common Criteria Evaluation Technical Report, Version 1.1, July 20, 2015, which is not publically available. The Assurance Activity Report, Version 1.1, July 20, 2015, provides a non-proprietary overview of testing and the prescribed assurance activities.

8.1 Evaluation Team Independent Testing

The evaluation Team verified the product in June 2015 at the vendor facility according to the Apriva MESA VPN Server Security Target, Version 0.10, July 15, 2015 document and ran the tests specified in the Protection Profile for Network Device Protection Profile Version 1.1, Security Requirements for Network Devices Errata #3, and Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1.

8.2 Vulnerability Analysis

8.2.1 NDPP

The evaluator began by searching cvedetails.com for the following search terms:

- Apriva
- VPN
- Mesa VPN
- RHEL 6
- NTP

The evaluator performed the searches listed above, and found several NTP and OpenSSL CVEs:

NTP

- http://www.cvedetails.com/cve/CVE-2014-9295/

OpenSSL

- http://www.cvedetails.com/cve/CVE-2014-3470/
- http://www.cvedetails.com/cve/CVE-2014-0224/
- http://www.cvedetails.com/cve/CVE-2014-0221/
- http://www.cvedetails.com/cve/CVE-2014-0195/

To determine whether the TOE is theoretically vulnerable to these attacks, the evaluator contacted the vendor and asked them to provide the versions of the OpenSSL and NTP packages. They stated that the TOE contains the following versions: openssl-1.0.1e-30.el6_6.8.x86_64, ntp-4.2.6p5-3.el6_6.x86_64, and ntpdate-4.2.6p5-3.el6_6.x86_64.

The evaluator found that the CVEs were addressed in previous RHEL package updates that are covered by the vendor's versions and are therefore not vulnerable:

- https://rhn.redhat.com/errata/RHSA-2014-0625.html
- https://rhn.redhat.com/errata/RHSA-2014-2024.html
- https://rhn.redhat.com/errata/RHBA-2015-0690.html

8.2.2 VPN

Based on discussions with TRRT and TD decisions, the evaluator reduced the scope of testing to the following components:

IPv4

- Type of Service
- Total Length
- Identification
- Flags
- Fragment Offset
- Time to Live
- Transport Layer Protocol

The evaluator used a script "fuzzIPv4.py" to perform fuzz testing and confirmed that no erratic or unusual behavior occurred on the TOE as a result of the fuzzing, and that the TOE dropped all traffic generated by the fuzzing tool. The tool fuzzes the IP length, IP flag, Type of Service, Time to Live, Protocol, Identification, and Fragment Offset.

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 the Protection Profile for Network Device Protection Profile, Version 1.1, June 8, 2012, Security Requirements for Network Devices Errata

#3, November 3, 2014, and Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, April 12, 2013. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in July 2015.

9.1 Clarifications of Scope

This evaluation only examines and proves the security claims contained within the Network Device Protection Profile and VPN Extended Package. The security claimed by this Common Criteria certification does not exceed the assurance provided by the evaluation activities defined by NIAP, and performed by the CCTL. In addition, this evaluation only covers the specific functionality defined within the Security Functional Requirements written in the NDPP and VPN EP. Though other functionality is included in the TOE, those features are not covered by this evaluation and are documented clearly in Section 4 and in the guidance documentation.

This evaluation only applies to the certified TOE: Apriva MESA VPN server 1.0, software version 21.16. Any other software version or hardware version is not covered by this certification process and no Common Criteria assurances can be claimed by a version other than the certified TOE.

In addition, the CCTL has only performed a vulnerability assessment within the scope of the AVA_VAN Security Assurance Requirement defined in the NDPP and VPN EP. This vulnerability assessment included IPv4 fuzzing and public domain vulnerability searches; only limited security can be claimed from the AVA_VAN analysis performed by the CCTL and should not be considered a substitute for an in-depth penetration test.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Security Target

Apriva MESA VPN Security Target, Version 0.10, July 15, 2015

12 Terms

12.1 Acronyms

Acronym	**Definition**
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratory
CD/DVD	Compact Disc / Digital Video Disc
CPU	Central Processing Unit
CSP	Critical Security Parameter
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
HMAC	Hash-based Message Authentication Code
I/O	Input/Output
IKEv2	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
ISS	Information Security Systems
IT	Information Technology
LLC	Limited Liability Company
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OS	Operating System
PCIe	Peripheral Component Interconnect (express)
PP	Protection Profile
RAM	Random Access Memory
RFC	Request for Comments
RHEL	RedHat Enterprise Linux

RSA	Rivest, Shamir, & Adleman
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
ST	Security Target
TCP	Transport Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
VPN	Virtual Private Network
VR	Validation Report

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.