National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Avaya Virtual Services Platform, Version 1.0

Report Number: CCEVS-VR-VID10755-2017

Dated: March 10, 2017

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin

Meredith Hennan

Marybeth Panock

The Aerospace Corporation

Common Criteria Testing Laboratory

Anthony Busciglio

Jatin Virmani

Dereck Oshin

Pascal Patin

Acumen Security, LLC

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. They should also carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Avaya Virtual Services Platform Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in March 2017. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for Collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015 (NDcPP).

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), as interpreted by the Assurance Activities contained in the Collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015 (NDcPP). 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 provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). 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). Based on these findings, 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.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Avaya Virtual Services Platform (VSP 4000, VSP 7000, VSP 8000)
Sponsor and Developer	Avaya, Inc. 4655 Great America Parkway, Santa Clara, CA 95054-1233
Common Criteria Testing Lab (CCTL)	Acumen Security 18504 Office Park Drive Montgomery Village, MD, 20886
Completion Date	March 10, 2017
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Protection Profile	Collaborative Protection Profile for Network Devices, Version 1.0
Disclaimer	This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.
Evaluation Personnel	Anthony Busciglio Jatin Virmani Dereck Oshin Pascal Patin *Acumen Security, LLC*
Validation Personnel	Daniel Faigin Meredith Hennan Marybeth Panock *The Aerospace Corporation*

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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 Compliance List.

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

Table 2: Evaluation Identifiers

Item	Identifier
Security Target Title and Version	Avaya Virtual Services Platform Common Criteria Security Target Document Version 1.6
Publication Date	March 2, 2017
Vendor	Avaya
Security Target Author	Acumen Security, LLC, Dean Freeman
Target of Evaluation Reference	Avaya Virtual Services Platform (VSP 4000, VSP 7000, VSP 8000)
TOE Software Version	5.1.2.0
Keywords	Network Device, Security Appliance

3 Architectural Information

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

3.1 TOE Overview

The TOE consists of a family of Ethernet switches that can be deployed in different environments to suit the needs of varying networks. They can be deployed individually or in combination with other solutions. The TOE also provides network protection through the use of industry standard security functions.

3.1.1 Virtual Services Platform 4000 Series: VSP 4850GTS, VSP 4850GTS-PWR+, VSP 4450GSX-PWR+

The VSP 4000 series are edge devices that are designed for small sites and delivers full-featured networking capabilities, while simplifying management by delivering multiple services without managing multiple protocols.

3.1.2 Virtual Services Platform 7000 Series: VSP 7024XLS 24-port 10GBASE-SFP+ Ethernet Switch, VSP 7024XT 24-port 10GBASE-T Ethernet Switch

The VSP 7000 series is a network device that can serve as a top rack switch, aggregate switch or core switch to improve network communications. The unique ability to alter the architecture of this series of switches makes it possible to solve many network challenges.

3.1.3 Virtual Services Platform 8000 Series: VSP 8284XSQ (fixed configuration), VSP 8404 4-slot Switch

The VSP 8000 series platform offer flexibility by including versatile network connectivity and the latest-generation hardware. The compact form-factor is an innovation that better power efficiency and allows for an easier way to increase port density.

3.2 TOE Evaluated Configuration

The TOE evaluated configuration consists of at least one of the following devices: VSP 4850GTS, VSP 4850GTS-PWR+, VSP 4450GSX-PWR+, VSP 7024XLS, VSP 7024XT, VSP 8284XSQ, and/or VSP 8404. The evaluated configuration also supports the following external IT entities;

Table 3: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation through remote CLI and GUI	Yes	This includes any IT Environment Management workstation with an SSH client and web browser installed that is used by the TOE administrator to support TOE administration through HTTPS and SSH protected channels.
NTP Server	No	The TOE optionally supports communications with an NTP server to synchronize date and time

Syslog Server	Yes	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.
Certificate Authority	Yes	The CA is used in support of certificate validation operations
OCSP Server	Yes	The OCSP server is used in support of certificate revocation testing.
AAA	Yes	This includes any IT environment AAA server that provides authentication services to TOE administration

4 Security Policy

4.1 Logical Boundaries

The TOE provides several areas of security functionality:

- Security Audit
- Cryptography Support
- Identification & Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channel

These features are described in more detail in the subsections below. In addition, the TOE implements all the SFRs and SARs of the Collaborative Protection Profile for Network Devices necessary to satisfy testing/ assurance measures prescribed therein.

4.2 Security Audit

The Network Appliances provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include the following: failure on invoking cryptographic functionality such as establishment, termination and failure of a TLS session; establishment, termination and failure of an SSH session; establishment, termination and failure of an IPsec session; all use of the user identification mechanisms; any use of the authentication mechanism; any change in the configuration of the TOE, changes to time, initiation of TOE update, indication of completion of TSF self-test, termination of a remote session; and initiation and termination of a trusted channel.

The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using SSH.

The logs for all of the appliances can be viewed via the remote GUI interface or through the CLI. The records include the date/time the event occurred, the event/type of event, the user ID associated with the event, and additional information of the event and its success and/or failure.

4.3 Cryptographic Support

The TOE provides cryptographic support for the following features,

- TLS/HTTPS connectivity with the following entities:
    - Management Web Browser
- SSH connectivity with the following entities:

    - Management SSH Client
    - Audit Server
- IPsec connectivity with the following entities:
    - AAA Server
- Secure software update

The cryptographic services provided by the TOE are described below.

Table 4: Provided Cryptography

Cryptographic Method	Use within the TOE	CAVP Certificate #
RSA Signature Services	• Used in TLS session establishment • Used in SSH session establishment • Used in IPsec session establishment • Used in secure software update	2219
SP 800-90A CTR_DRBG	• Used in TLS session establishment • Used in SSH session establishment • Used in IPsec session establishment	1232
SHS	• Used to provide TLS traffic integrity verification • Used to provide SSH traffic integrity verification • Used to provide IPsec traffic integrity verification • Used in secure software update	3375
HMAC-SHS	• Used to provide TLS traffic integrity verification • Used to provide SSH traffic integrity verification • Used to provide IPsec traffic integrity verification	2679
AES	• Used to encrypt TLS traffic • Used to encrypt SSH traffic • Used to encrypt IPsec traffic	4100
SP 800-56A	• Used in TLS session establishment • Used in SSH session establishment • Used in IPsec session establishment	971
DSA	• Used in support of SP 800-56A	1140
Note: The TOE runs Mentor Graphics Linux 4.0		

4.4 Identification and Authentication

The TOE provides authentication services for administrative users to connect to the TOEs administrator interfaces (local CLI, remote CLI, and remote GUI). The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. In the Common Criteria evaluated configuration, the TOE is configured to require a minimum password length of 15 characters. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on any TOE administrative interface either locally or via an AAA server.

4.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. Management can take place over a variety of interfaces including:

- Local console command line administration at each of the appliances.
- Remote command line administration via SSHv2 at each appliance.
- Remote GUI administration via HTTPS/TLS.

The TOE provides multiple interfaces to perform administration. While in the CLI command mode, the user has access to six distinct modes that provide a specific set of commands. Higher modes can mostly access commands of the lower modes, except, if they conflict with commands of the current mode. The CLI modes are as follows;

- User EXEC Mode: Initial mode of access.
- Privileged EXEC Mode: User mode and password combination determines access level.
- Global Configuration Mode: Use this mode to make changes to the running configuration.
- Interface Configuration Mode: Use this mode to modify or configure logical interface, VLAN or a physical interface.
- Router Configuration Mode: Use this mode to modify a protocol.
- Application Configuration Mode: Use this mode to access the applications.

The TOE also offers a web-based graphical user interface in order to securely manage the appliances. This is known as the Enterprise Device Manager (EDM) and is accessible once it has been enabled through the CLI.

All administration functions can be accessed via, remote CLI, remote GUI or via a direct connection to the TOE. The TOE provides the ability to securely manage the following:

- All TOE administrative users
- All identification and authentication
- All audit functionality of the TOE
- All TOE cryptographic functionality
- The timestamps maintained by the TOE
- Update to the TOE

The TOE supports the configuration of login banners to be displayed at time of login and inactivity timeouts to terminate administrative sessions after a set period of inactivity.

4.6 Protection of the TSF

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

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually, or can configure the TOE to use NTP to synchronize the TOE's clock with an external time source. Finally, the TOE performs testing to verify correct operation of the security appliances themselves. The TOE verifies all software updates via digital signature (2048-bit RSA/SHA-256) and requires administrative intervention prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

4.7 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE can also display an Authorized Administrator specified banner on both the CLI and GUI management interfaces prior to allowing any administrative access to the TOE.

4.8 Trusted Path/Channels

The TOE supports the following types of secure communications:

- Trusted paths with remote administrators over SSH
- Trusted paths with remote administrators over TLS/HTTPS
- Trusted channels with remote IT environment audit servers over SSH
- Trusted channels with remote IT environment AAA servers over IPsec

5 Security Problem Definition

5.1 Threats

The following section lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

5.1.1 Communications with the Network Device

A network device communicates with other network devices and other network entities. The endpoints of this communication can be geographically and logically distant and may pass through a variety of other systems. The intermediate systems may be untrusted providing an opportunity for unauthorized communication with the network device or for authorized communication to be compromised. The security functionality of the network device must be able to protect any critical network traffic (administration traffic, authentication traffic, audit traffic, etc.). The communication with the network device falls into two categories: authorized communication and unauthorized communication.

Authorized communication includes network traffic allowable by policy destined to and originating from the network device as it was designed and intended. This includes critical network traffic, such as network device administration and communication with an authentication or audit logging server, which requires a secure channel to protect the communication. The security functionality of the network device includes the capability to ensure that only authorized communications are allowed and the capability to provide a secure channel for critical network traffic. Any other communication is considered unauthorized communication.

The primary threats to network device communications addressed in this cPP focus on an external, unauthorized entity attempting to access, modify, or otherwise disclose the critical network traffic. A poor choice of cryptographic algorithms or the use of non-standardized tunneling protocols along with weak administrator credentials, such as an easily guessable password or use of a default password, will allow a threat agent unauthorized access to the device. Weak or no cryptography provides little to no protection of the traffic allowing a threat agent to read, manipulate and/or control the critical data with little effort. Non-standardized tunneling protocols not only limit the interoperability of the device but lack the assurance and confidence standardization provides through peer review.

5.1.1.1 T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

5.1.1.2 T.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

5.1.1.3 T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

5.1.1.4 T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

5.1.2 Valid Updates

Updating network device software and firmware is necessary to ensure that the security functionality of the network device is maintained. The source and content of an update to be applied must be validated by cryptographic means; otherwise, an invalid source can write their own firmware or software updates that circumvents the security functionality of the network device. Methods of validating the source and content of a software or firmware update by cryptographic means typically involve cryptographic signature schemes where hashes of the updates are digitally signed.

Unpatched versions of software or firmware leave the network device susceptible to threat agents attempting to circumvent the security functionality using known vulnerabilities. Non-validated updates or updates validated using non-secure or weak cryptography leave the updated software or firmware vulnerable to threat agents attempting to modify the software or firmware to their advantage.

5.1.2.1 T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

5.1.3 Audited Activity

Auditing of network device activities is a valuable tool for administrators to monitor the status of

the device. It provides the means for administrator accountability, security functionality activity reporting, reconstruction of events, and problem analysis. Processing performed in response to device activities may give indications of a failure or compromise of the security functionality. When indications of activity that impact the security functionality are not generated and monitored, it is possible for such activities to occur without administrator awareness. Further, if records are not generated and retained, reconstruction of the network and the ability to understand the extent of any compromise could be negatively affected. Additional concerns are the protection of the audit data that is recorded from alteration or unauthorized deletion. This could occur within the TOE, or while the audit data is in transit to an external storage device.

Note this cPP requires that the network device generate the audit data and have the capability to send the audit data to a trusted network entity (e.g., a syslog server).

5.1.3.1 T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.

5.1.4 Administrator and Device Credentials Data

A network device contains data and credentials which must be securely stored and must appropriately restrict access to authorized entities. Examples include the device firmware, software, configuration authentication credentials for secure channels, and administrator credentials. Device and administrator keys, key material, and authentication credentials need to be protected from unauthorized disclosure and modification. Furthermore, the security functionality of the device needs to require default authentication credentials, such as administrator passwords, be changed.

Lack of secure storage and improper handling of credentials and data, such as unencrypted credentials inside configuration files or access to secure channel session keys, can allow an attacker to not only gain access to the network device, but also compromise the security of the network through seemingly authorized modifications to configuration or though man-in-the-middle attacks. These attacks allow an unauthorized entity to gain access and perform administrative functions using the Security Administrator's credentials and to intercept all traffic as an authorized endpoint. This results in difficulty in detection of security compromise and in reconstruction of the network, potentially allowing continued unauthorized access to administrator and device data.

5.1.4.1 T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.

5.1.4.2 T.PASSWORD_CRACKING

Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.

5.1.5 Device Failure

Security mechanisms of the network device generally build up from roots of trust to more complex sets of mechanisms. Failures could result in a compromise to the security functionality of the device. A network device self-testing its security critical components at both start-up and during run-time ensures the reliability of the device's security functionality.

5.1.5.1 T.SECURITY_FUNCTIONALITY_FAILURE

A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

5.2 Assumptions

This section describes the assumptions made in identification of the threats and security requirements for network devices. The network device is not expected to provide assurance in any of these areas, and as a result, requirements are not included to mitigate the threats associated. The section that follows describes the security objectives that are expected to be provided by the operational environment to mitigate these threats.

5.2.1 A.PHYSICAL_PROTECTION

The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. [OE.PHYSICAL]

5.2.2 A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality). [OE.NO_GENERAL_PURPOSE]

5.2.3 A.NO_THRU_TRAFFIC_PROTECTION

A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is

destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall).[OE.NO_THRU_TRAFFIC_PROTECTION]

5.2.4 A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device. [OE.TRUSTED_ADMIN]

5.2.5 A.REGULAR_UPDATES

The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities. [OE.UPDATES]

5.2.6 A.ADMIN_CREDENTIALS_SECURE

The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside. [OE.ADMIN_CREDENTIALS_SECURE]

5.3 Security Objectives for the Operational Environment

5.3.1 OE.PHYSICAL

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

5.3.2 OE.NO_GENERAL_PURPOSE

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

5.3.3 OE.NO_THRU_TRAFFIC_PROTECTION

The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

5.3.4 OE.TRUSTED ADMIN

TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.

5.3.5 OE.UPDDATES

TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

5.3.6 OE.ADMIN_CREDENTIALS_SECURE

The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

5.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 level of assurance for this evaluation is defined within the Collaborative Protection Profile for Network Devices, Version 1.0 (NDcPP).
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Avaya Virtual Services Platforms Common Criteria Security Target, version 1.6, 3 March 2017
- Common Criteria Avaya VSP Series Addendum, version 1.5, 10 March 2017
- Avaya VSP4000, VSP 7000 and VSP 8000 Appliances Entropy Assessment Report, version 1.2, 22 August 2016

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Avaya Virtual Services Platform (VSP 4000, VSP 7000, VSP 8000), which is not publically available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

7.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the Collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015 (NDcPP). The Independent Testing activity is documented in the Assurance Activities Report, which is publically available, and is not duplicated here. The testbed diagram that was used appears below.

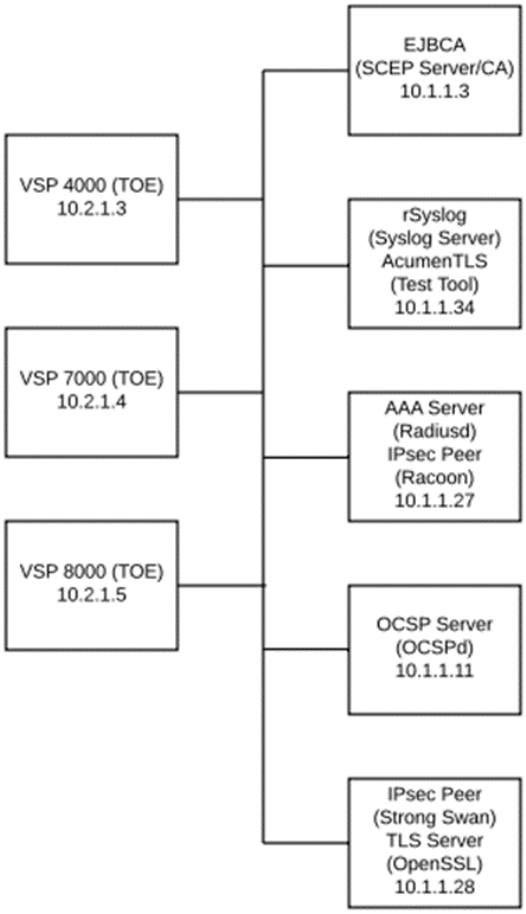

Figure 1 Testbed Diagram

8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: The Test Report (TR) and the Evaluation Technical Report (ETR). The reader of this document can assume that 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 that the Avaya VSP 4000 series, Avaya VSP 7000 series and Avaya VSP 8000 series to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the Collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015 (NDcPP).

8.1 Evaluation of Security Target

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 Avaya VSP 4000 series, Avaya VSP 7000 series and Avaya VSP 8000 series are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the NDcPP.

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.

8.2 Evaluation of Development Documentation

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's TOE Summary Specification. The evaluation team applied each applicable ADV CEM work unit. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities and the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.3 Evaluation of Guidance Documents

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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. The evaluation team applied each applicable AGD CEM work unit. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities and the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.4 Evaluation of Life Cycle Support Activities

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

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.

8.5 Evaluation of Test Documentation and the Test Activity

The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report. The evaluation team also applied each applicable ATE CEM work unit.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP and the assurance activities called out in the CEM, and that the conclusion reached by the evaluation team was justified.

8.6 Vulnerability Assessment Activity

The evaluation team applied each applicable AVA CEM work unit. The evaluation team performed vulnerability testing and conducted web searches for vulnerabilities that could potentially affect the TOE. The web searches were conducted on the public Internet and on the National Vulnerabilities Database (http://nvd.nist.gov/). No issues were discovered

The evaluator performed the public domain vulnerability searches using the following key words.

- Avaya VSP
- VSP

- VOSS 5.1.2
- TLS 1.2
- Mocana
- Mocana Cryptographic Suite B
- Mentor Graphics Linux
- Yocto Project
- Wind River Linux

The evaluator selected the search key words based upon the following criteria.

- The vendor name was searched
- The software running on the TOE devices were searched. Further, the version the TOE software in evaluation was searched
- The name of the hardware devices within the TOE
- The secure protocols supported by the TOE
- The type of TOE device

As Mentor Graphics Linux the OS running on the TOE is a secure custom kernel Linux distribution based on the Yocto Project, akin to the Wind River Linux. Therefore, Mentor Graphics Linux, Yocto Project, and WindRiver Linux were all included as part of the vulnerability search. Note that some Avaya products rebrand Mentor Graphic Linux as VOSS; hence VOSS was also included in the search.

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 addressed the vulnerability analysis Assurance Activities in the NDcPP and the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.7 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 test activities 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 performed the Assurance Activities in the NDcPP and the work units defined in the CEM, and correctly verified that the product meets the claims in the ST.

9 Validator Comments & Recommendations

- The validation team's observations support the evaluation team's conclusion that the Avaya Virtual Services Platform meets the claims stated in the Security Target.
- The evaluation documentation, e.g., the Security Target, the Common Criteria Guidance, the Assurance Activity Report, identify the TOE OS as Mentor Graphics Linux 4.0. However, the commercial documentation available on the Avaya website identifies Mentor Graphics Linux as VOSS when referring to the operating system of the Avaya Virtual Service Platforms. VOSS is a rebranding of Mentor Graphics Linux and during the course of the evaluation an equivalency argument was provided which stated that these two versions of Linux are identical. This argument was accepted by NIAP. The CAVP certs specify Mentor Graphics Linux while the evaluation testing was conducted on the OS identified as VOSS. Additionally, it was confirmed that the FIPS lab had used the same equipment to generate the evidence for the certificates as the CCTL used for product testing. VOSS and Mentor Graphics are the same Operating System.
- The collaborative Protection Profile for Network Devices allows the selection of "drop new audit data" when the local storage space for audit data is full. It may be permissible, but is not likely to meet the objective nor provide the accountability the end customer needs. It is one thing to overwrite the oldest audit data, as that means you always have the latest activity. But writing over the newest or stopping auditing does not provide accountability. The TSS states that audit records are stored in a log file which stops keeping records if the log becomes full. Only authorized administrators are able to clear audit logs, but they cannot modify them. This means that the authorized administrators need to monitor the audit log storage to ensure that audit logs are not lost.
- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance via the invocation of the assurance activities specified in the relevant Collaborative Protection Profile for Network Devices.
- This evaluation covers only the software and hardware as identified in this document, no earlier or later versions.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Network Device collaborative Protection Profiles; any additional security related functionality outside that specified was not covered by this evaluation.
- Any documentation in addition to that listed in this Validation Report was not included in the evaluation and therefore should not be relied upon when configuring or using the product in its evaluated configuration.

10 Annexes

Not applicable.

11 Security Target

Avaya Virtual Services Platforms, Common Criteria Security Target, Version 1.6

12 Glossary

- **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.

13 Acronym List

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
CLI	Command Line Interface
DRBG	Dynamic Random Bit Generator
DSA	Digital Signature Algorithm
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
IPsec	Internet Protocol Security
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
NVLAP	National Voluntary Laboratory Assessment Program
OCSP	Online Certificate Status Protocol
OS	Operating System
PCL	Products Compliant List
RSA	Rivest Shamir Adelman
SHS	Secure Hash Standard
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report
VSP	Virtual Services Platform

14 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, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
4. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CCMB-2012-09-004, Version 3.1 Revision 4, September 2012
5. Avaya Virtual Services Platforms Common Criteria Security Target, version 1.6, 3 March 2017
6. Common Criteria Avaya VSP Series Addendum, version 1.5, 3 March 2017
7. Common Criteria NDcPP Assurance Activity Report for Avaya Virtual Services Platforms, version 1.8, 9 March 2017
8. VID 10755 AVAYA VSP Equivalency Analysis, version 1.0, 30 August 2016
9. Avaya VSP4000, VSP 7000 and VSP 8000 Appliances Entropy Assessment Report, version 1.2, 22 August 2016 [Acumen Security and Avaya Confidential]
10. Avaya Virtual Services Platform Security Target Evaluation Technical Report, version 1.4, 3 March 2017
11. Avaya VSP Evaluation Technical Report. Version 1.0 10 March 2017
12. Test Report for Avaya VSP 4450GSX-PWR+, Version 4.0, 3 March 2017 [Acumen Security and Avaya Confidential]
13. Test Report for Avaya VSP 7024XLS, Version 3.0, 3 March 2017 [Acumen Security and Avaya Confidential]
14. Test Report for Avaya VSP 48284XSQVersion 3.0, 3 March 2017 [Acumen Security and Avaya Confidential]