National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

VMware Avi Load Balancer, Version 30.2.3

Report Number: CCEVS-VR-VID11491-2025

Dated: May 8, 2025

Version: 1.3

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Chris Thorpe

The MITRE Corporation

Farid Ahmed

Robert Wojcik
Russ Fink

Johns Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

Saniya Shaikh
Akshay Jain
Rupendra Kadtan
Guruprasad Sawant
Rahul Joshi (Lead Evaluator)

Intertek Acumen Security

Table of Contents

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. Prospective users should 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 VMware Avi Load Balancer, Version 30.2.3 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 May 2025. 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 of the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND].

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR 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 ETR 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 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 ETR are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (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 IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	VMware Avi Load Balancer, Version 30.2.3
Protection Profile	Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND]
Security Target	VMware Avi Load Balancer, Version 30.2.3 Security Target, Version 1.2
Evaluation Technical Report	Evaluation Technical Report for VMware Avi Load Balancer, Version 30.2.3, Version 0.6.
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Broadcom
Developer	Broadcom
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	 Chris Thorpe Farid Ahmed Robert Wojcik Russ Fink

3 Architectural Information

3.1 TOE Description

The TOE is VMware Avi Load Balancer Version 30.2.3 which is a network device running as VMware ESXi based Virtual Machine. The TOE is a distributed software TOE consisting of the VMware Avi Controller (hereafter referred to as Controller) and the VMware Avi Service Engine (hereafter referred to as SE). The software-defined, scale-out architecture provides on-demand autoscaling of elastic load balancers. The distributed software load balancers and the backend applications can scale up or down in response to real-time traffic monitoring. Application load balancing becomes more adaptable and intelligent.

The TOE is a distributed virtual TOE comprised of two components:

1. AVI controller (Controller) – The Controller is the "brain" of the entire system and acts as a single point of intelligence, management, and control across a distributed fabric of enterprise-grade load balancers. The Controller is a virtual machine based on Ubuntu Server 20.04 running on a VMware ESXi 7.0.3 hypervisor with an Intel Xeon Gold 6126 processor.
2. Service Engine (SE) – The SE is the distributed data plane. The SE is a virtual machine based on Ubuntu Server 20.04 running on a VMware ESXi 7.0.3 hypervisor with an Intel Xeon Gold 6126 processor.

3.2 Sample TOE Deployment

The following figure represents a sample TOE deployment:

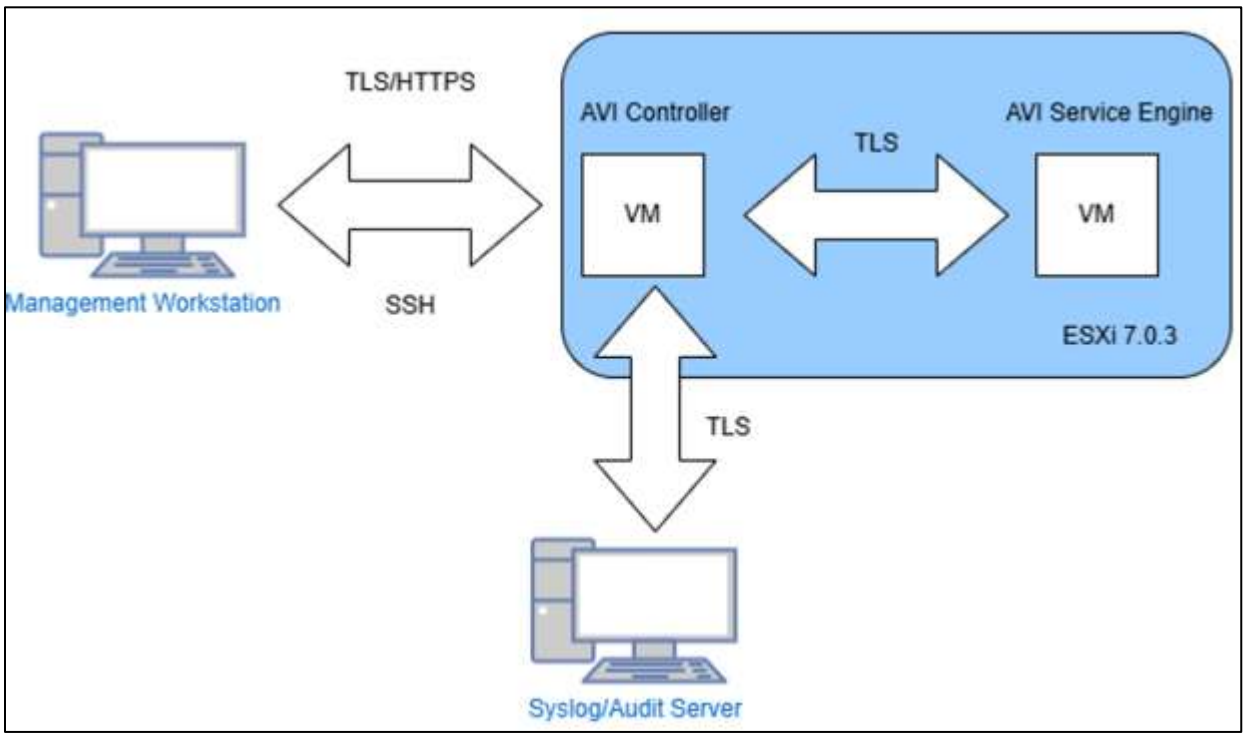

Figure 1 – Representative TOE Deployment

3.3 Physical Boundaries

The physical boundaries of the distributed TOE components are described as follows:

- Avi Controller, virtual machine deployed on ESXi 7.0.3
- Avi Service Engine, virtual machine deployed on ESXi 7.0.3

The Controller and SE components are vNDs as defined in Case 1 of PP-ND. The ESXi 7.0.3 hypervisor and underlying hardware platform are part of the evaluated configuration but not included in the TOE boundary.

3.4 TOE Evaluated Platform

Detail regarding the evaluated platform is provided in Section 7 below.

4 Security Policy

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as PP-ND v2.2e or PP-ND.

4.1 Security Audit

The Controller is capable of generating audit records and maintaining a local storage which is rotated when the buffer becomes full. The SE component generated audit records and maintains them temporarily in a local buffer until it has been transferred to the Controller. The Controller component sends its audit records directly to an external syslog server over a trusted channel protected with TLS. The SE component sends its audit records to the Controller component over TLS.

4.2 Cryptographic Support

The Controller and the SE performs cryptographic functions including key generation and key establishment, symmetric encryption and decryption, hashing, keyed hash message authentication, digital signatures, and random number generation. The following cryptographic libraries is used in support of this functionality:

- VMware's OpenSSL FIPS Object Module

These cryptographic modules were validated on Ubuntu Server 20.04 with ESXi v7.0.3 on an Intel Xeon Gold 6126 processor. The CAVP algorithm certificate details are provided in Section 6.1.

The Controller and the SE cryptographic functionality is implemented in support of TLS v1.2 server (HTTPS) and client (Syslog over TLS) functionality, as necessary to support trusted path and channel functions. Additionally, Controller provides SSHv2 server functionality for remote administration necessary to support trusted path and serves as a trusted channel for manual update functions.

4.3 Identification and Authentication

Remote and local administrators are authenticated via the Controller component. Repeated failed remote authentications will lock the administrative account after a configurable threshold of attempts. Locked accounts are re-enabled after a configurable time period or can be re-enabled by another administrator. Passwords must meet a configurable minimum length and may be composed of upper-case and lower-case letters, numbers, and special characters. No functionality is available prior to successful authentication. Password characters are obscured during entry.

The Controller and SE components support X.509v3 certificate authentication and revocation checking for the following purposes:

- Validation of a syslog server TLS certificate (Controller).

The Controller is capable of generating certificate signing requests in support of authentication in the following scenarios:

- The Controller TLS server authentication for remote administration and internal distributed TOE communication.

- The SE component also validates the Controller TLS server certificate used for internal distributed TOE channel. Certificate revocation is not supported for the distributed TOE channel.

4.4 Security Management

The Controller is the primary management component of the TOE and supports local management via VMware console connection as well as remote management via an HTTPS/TLS Web UI and SSH CLI. The following functionality is available and restricted to authorized security administrators:

- Administer the TOE locally and remotely.
- Configuration of the access banner.
- Configuration of the session inactivity timeouts.
- Performing manual TOE updates.
- Configuring the authentication failure parameters.
- Start and stop services.
- Configuring the transmission of audit data to an external server.
- Management of cryptographic keys.
- Configure the cryptographic functionality.
- Configuring the communication between the Controller and the SE.
- Setting the system time.
- Configure NTP.
- Manage the TOE's trust store and designate X509.v3 certificates as trust anchors.
- Import X.509v3 certificates to the TOE's trust store.
- Manage the trusted public keys database.

4.5 Protection of the TSF

Administrative passwords are stored in the filesystem of the Controller and are protected via a salted hash. Private keys are stored in the Controller filesystems and public keys are stored in the SE and neither is readable through any TOE interface.

The Controller and SE communicate via an internal trusted channel usingTLS.

The system clocks of the Controller and SE components are set manually by the security administrator in support of reliable time stamps. The security administrator can also synchronise time with an NTP server.

The Controller and SE components perform a suite of cryptographic known algorithm tests, entropy noise source tests, and a digital signature-based integrity test of the TOE executable code during startup. In the event of a failure of any of the required self-tests, the TOE will shut down its operations until the error can be recovered.

Updates are verified and installed manually by the TOE security administrator using a published hash value.

4.6 TOE Access

The Controller terminate local administrative sessions after a configurable time period of inactivity.
The Controller terminate a remote administrative session after a configurable time period of inactivity.

Administrators may terminate their own session by issuing a 'logout' command from either the remote CLI or GUI.

Prior to authenticating to the local CLI or the remote CLI or GUI, the administrator is presented with a configurable advisory notice and consent message.

4.7 Trusted Path/Channels

The TOE acts as a server for the following communications

- HTTPS server (Controller remote administration)
- SSH server (Controller CLI remote administration)
- TLS server (Controller to SE trusted channel)

The TOE acts as a client for the following communications:

- TLS client (Controller syslog)
- TLS client (SE to Controller trusted channel)

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 2 – Assumptions

ID	Assumption
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 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 does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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. For vNDs, this assumption applies to the physical platform on which the VM runs.
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 a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.

ID	Assumption
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 and PP-Modules for particular types of Network Devices (e.g., firewall).
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 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. (The paragraph that follows is for x509v3 cert-based authentication. If not relevant, remove) For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
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.
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.

ID	Assumption
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_ADMINISTRATOR	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATION (applies to vNDs only)	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

5.2 Threats

The following table 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.

Table 3 – Threats

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means

ID	Threat
	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.
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.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling 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.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the

ID	Threat
	device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
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.
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 includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
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.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

5.3 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 2.2e, 23 March 2020 [PP-ND].

- Consistent with the expectations of the PP, 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:

- VMware Avi Load Balancer, Version 30.2.3 Security Target, Version 1.2 [ST]
- VMware Avi Load Balancer, Version 30.2.3 Administration Manual for Common Criteria, Version 0.6 [AGD]

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE was evaluated based on a representative TOE deployment delineated in Figure 1.

The physical boundaries of the distributed TOE components are described as follows:

- Avi Controller, virtual machine deployed on ESXi 7.0.3
- Avi Service Engine, virtual machine deployed on ESXi 7.0.3

The Controller and SE components are vNDs as defined in Case 1 of PP-ND. The ESXi 7.0.3 hypervisor and underlying hardware platform are part of the evaluated configuration but not included in the TOE boundary.

7.2 Testing Environment and Configuration

Figure 2 below shows the TOE testing environment overview

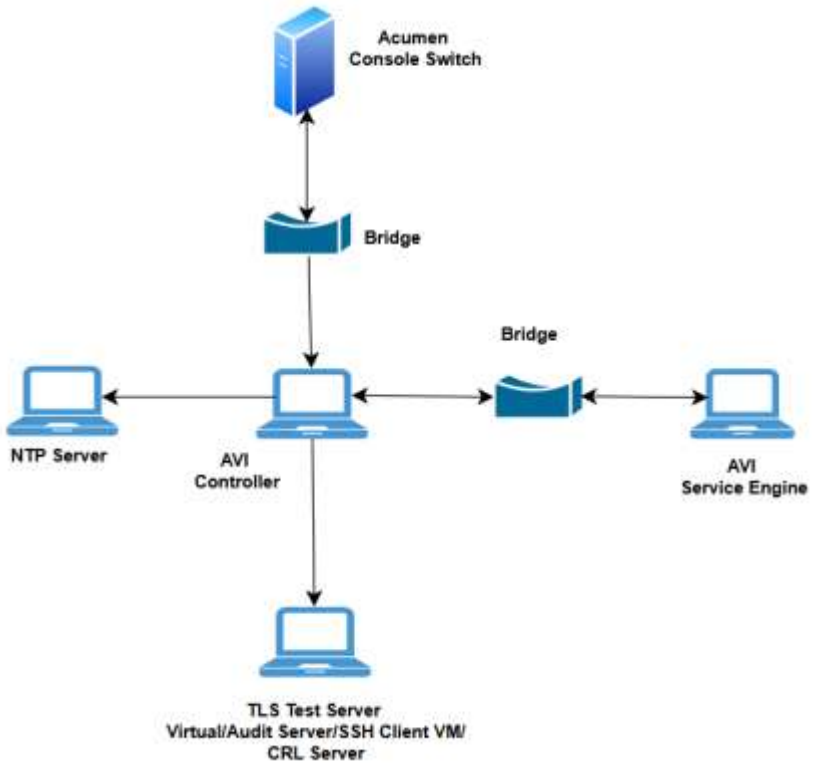

Figure 2 –TOE Testing Environment

The following table provides configuration information about each device in the test environment.

Table 4 – Configuration of the Testing Environment

Device Details		System Details			
Device Name	**Function**	**Protocols**	**OS, including version**	**Timing Source**	**Software & Tools, including version**
Avi Controller	TOE	TLS, HTTP, and SSH	Ubuntu Server 20.04	Using the NTP server.	N/A
Avi Service Engine (SE)		SSH, TLS	Ubuntu Server 20.04	Using the NTP server.	N/A
Acumen Console Switch	Console	N/A	IOS XE	Using the NTP server.	N/A
TLS Test Server Virtual/ Audit Server/SSH Client VM/CRL Server	Audit Server	SSH, TLS	Ubuntu 18.04	Using the NTP server.	MITM Tool, OpenSSL, rsyslogd, acumen-tlsc-v2.2e, acumen-tls, X509-mod, Wireshark, strongswan
Test VM	NTP Server	NTP	Ubuntu 18.04	Using the NTP server.	Wireshark, OpenSSL
Bridge 1	Bridge	N/A	N/A	N/A	N/A
Bridge 2	Bridge	N/A	N/A	N/A	N/A

7.3 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- High Availability
- Load Balancing
- Orchestrator
- Automation
- Analytics
- Scaling

8 Scaling IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for VMware Avi Load Balancer 30.2.3, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

9 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 Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all 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. (5) and CEM version 3.1 Rev. (5). The evaluation determined the TOE Name 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 2.2e, 23 March 2020 [PP-ND].

9.1 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 VMware Avi Load Balancer 30.2.3 that 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 Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND].

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.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND] 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 that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND] 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 that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND] and recorded the results in a Test Report, summarized in the ETR and AAR.

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 Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND], and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

Following sources were searched during the evaluation:

- https://nvd.nist.gov/view/vuln.search
- http://cve.mitre.org/cve
- https://support.broadcom.com/web/ecx/security-advisory

The searches were performed on April 29, 2025 with the following keywords:

- Load Balancer
- VMware Avi Load Balancer
- VMware Avi Service Engine
- VMware Avi Controller
- VMware's OpenSSL FIPS Object Module
- AVI Controller
- AVI Service engine
- cpe:/:intel:xeon_gold_6126:- (Intel Xeon Gold 6126)
- cpe:/:canonical:ubuntu_linux:20.04 (Ubuntu 20.04)
- openssl 1.0.2z

- cpe:/:openbsd:openssh:8.2 (openssh-8.2p1-4ubuntu0.12)
- cpe:/:net-snmp:net-snmp:5.9.3
- nginx-1.18.0
- cpe:/:haxx:curl:8.9.1 (curl-8.9.1)
- iptables-1.8.4
- boringcrypto
- bind9-dnsutils 9.16.48
- cpe:/:vmware:esxi:7.0

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 Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND], and that the conclusion reached by the evaluation team was justified.

9.7 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 Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND], and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the configuration guide document listed in Section 6. No other versions of the TOE, either earlier or later, were evaluated. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. See Section 7.3 of this report for product functionality that is not included in the scope of evaluation. Additional functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Annexes

Not applicable.

12 Security Target

VMware Avi Load Balancer, Version 30.2.3 Security Target, Version 1.2 [ST]

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

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, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Assurance Activity Report for VMware Avi Load Balancer, Version 30.2.3, Version 1.6
6. Evaluation Technical Report for VMware Avi Load Balancer, Version 30.2.3, Version 0.6
7. VMware Avi Load Balancer Version 30.2.3 Administration Manual for Common Criteria, Version 0.6
8. Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND]
9. VMware Avi Load Balancer, Version 30.2.3 Security Target, Version 1.2.