National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

VMware NSX-T Data Center 3.1

Report Number: CCEVS-VR-VID11217-2022

Dated: 22 July 2022

Version: 1.0

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 Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jerome F Myers

Swapna Katikaneni

Mike Quintos

Aerospace Corporation

Common Criteria Testing Laboratory

Riya Thomas

Yogesh Pawar

Kenneth Lasoski

Acumen Security, LLC

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 NSX-T Data Center 3.1 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 **July 2022**. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security as summarized in the Assurance Activity Report (AAR) for VMware NSX-T Data Center 3.1. 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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP].

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP] and all applicable NIAP technical decisions for the technology. 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 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 AAR. The validation team found that the evaluation showed that the product satisfies all 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 Protection Profiles (PPs) containing Assurance Activities, which are interpretations 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 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 Compliance List.

The TOE is the VMware NSX-T Data Center 3.1 and the associated TOE guidance documentation.

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.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	VMware NSX-T Data Center 3.1
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]
Security Target	VMware NSX-T Data Center 3.1 Common Criteria Security Target Version 1.6
Evaluation Technical Report	Evaluation Technical Report for VMware NSX-T Data Center 3.1
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	VMware, Inc.
Developer	VMware, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security, LLC
CCEVS Validators	Jerome F Myers Swapna Katikaneni Mike Quintos

Table 1 – Identification

3 Architectural Information

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

The Target of Evaluation (TOE) is VMware NSX-T Data Center 3.1, a VMware network device software product that provides and manages virtual networking components. The TOE is designed as a network virtualization platform, providing the ability to implement and virtualize networks across multiple ESXi nodes and virtual machines (VMs).

For the purpose of testing of the identified TOE, the evaluated TOE configuration is as followings: VMware NSX-T Data Center 3.1 on hypervisor VMware ESXi 6.7 running Ubuntu 18.04 on Dell Power Edge R740 with Intel Xeon Gold 6230R (Cascade Lake).

The TOE provides functionality to enforce and support auditing, cryptographic operations, network separation, encrypted channels, identification/authentication, security management, and protection of the TSF. Administrators can configure virtual network.

In VMware's network virtualization solution, the following components are the essential building blocks that make up the virtualized computing environment:

- NSX-T Unified Appliance is a virtual appliance configured to run NSX-T application roles (Manager, Policy, and Controller).
- The NSX-T Edge is a virtual appliance that provides routing services and connectivity to networks that are external to the NSX-T deployment.

The components described above make a basic virtualized environment ready for virtualized networking. The NSX-T Unified Appliance provides a single API entry point to the system, persists user configuration, handles user queries, and performs operational tasks. The TOE is configured for a single instance of ESXi 6.7 Hypervisor, which includes a single NSX-T Unified Appliance instance, and a single instance of the NSX-T Edge appliance.

TOE supports both local and remote administration. The TOE provides a local console interface which supports CLI. REST API over TLS is the remote interface.

.

4 Security Policy

The TOE is comprised of several security features, as identified below:

Logical Boundary Rationale for Security Audit (FAU)

Security Function	Description
Security Audit (FAU)	The TOE generates audit records for all security-relevant events. For each audited events, the TOE records the date and time, the type of event, the subject identity, and the outcome of the event. The resulting records are stored on Unified Appliance and can be sent securely to a designated log server for archiving. Security Administrators, using the appropriate REST API commands, can also view audit records locally. The TOE provides a reliable timestamp relying on the appliance's to built-in clock.

Logical Boundary Rationale for Cryptographic Support (FCS)

Security Function	Description
Cryptographic Support (FCS)	The TOE provides cryptography support for secure communications and protection of information. The cryptographic services provided by the TOE are listed in Table 3 - TOE Provided Cryptography below. The TOE implements the secure protocols - TLS/HTTPS on the server side and TLS on the client side. The TOE implements deletion procedures to mitigate the possibility of disclosure or modification of CSPs. The TOE uses two types of dedicated cryptographic modules to manage CSPs: VMware BC-FJA (Bouncy Castle FIPS Java API) module for Java based implementations of TLS/HTTPS, key stores, and trust stores; and VMware's OpenSSL FIPS Object module for TLS/HTTPS, key stores, and trust stores. The algorithm certificate references are listed in the tables below (Table 4 – VMware's OpenSSL FIPS Object Module Algorithm and Table 5 – VMware BC-FJA (Bouncy Castle FIPS Java API) Module Algorithm) described in the ST.

The following table lists all cryptography provided within TOE:

Cryptographic Method	Usage within the TOE
TLS Establishment	Used to establish initial TLS session
ECDH Key Agreement	Used in TLS session establishment
RSA Key Generation	Used to create key-pairs and X.509 certificates for use in TLS protocols
RSA Signature Services	Used in TLS session establishment. Used in secure software update
SP 800-90 DRBG	Used in TLS session establishment
SHS	Used in secure software update
HMAC-SHS	Used to provide TLS traffic integrity verification
AES	Used to encrypt TLS traffic

Table 2 – TOE Provided Cryptography

Algorithms under VMware's OpenSSL FIPS Object Module cryptography module are listed in the table:

Algorithm	Description	Mode Supported	CAVP Cert. #	Standards
AES	Used for symmetric encryption/decryption	GCM (128 and 256 bits) CBC (128 and 256 bits)	A1292	SP 800-38D SP 800-38A
SHS (SHA)	Cryptographic hashing services	Byte Oriented SHA-1, SHA-256, SHA-384	A1292	FIPS 180-4
HMAC	Keyed hashing services and software integrity test	Byte Oriented HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	A1292	FIPS 198
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	Hash_DRBG (512) CTR_DRBG (AES-256)	A1292	SP 800-90A
RSA	Signature Generation and Verification	FIPS PUB 186-4 Key Generation (2048-bit, 3072 bit key)	A1292	FIPS 186-4
CVL – KAS-ECC	Key Agreement	NIST Special PUB 800-56A	A1292	SP 800-56Ar3

Table 3 – VMware's OpenSSL FIPS Object Module Algorithm

Algorithm	Description	Mode Supported	CAVP Cert. #	Standards
AES	Used for symmetric encryption/decryption	GCM (128 and 256 bits) CBC (128 and 256 bits)	C2174	SP 800-38D SP 800-38A
SHS (SHA)	Cryptographic hashing services	Byte Oriented SHA-1, SHA-256, SHA-384	C2174	FIPS 180-4
HMAC	Keyed hashing services and software integrity test	Byte Oriented HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	C2174	FIPS 198
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	Hash_DRBG (512) CTR_DRBG (AES-256)	C2174	SP 800-90A
RSA	Signature Generation and Verification	FIPS PUB 186-4 Key Generation (2048-bit, 3072 bit key)	C2174	FIPS 186-4
CVL – KAS-ECC	Key Agreement	NIST Special Publication 800-56A	C2174	SP 800-56Ar3

Table 4 – VMware BC-FJA (Bouncy Castle FIPS Java API) Module Algorithm

Logical Boundary Rationale for Identification and Authentication (FIA)

Security Function	Description
Identification and Authentication (FIA)	Security Administrators are identified and authenticated prior to being allowed access to any of the services other than the display of the warning banner. The REST API requires user name and password for authentication. The identification and authentication credentials are confirmed against a local user database. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS/HTTPS connections. The TOE provides the capability to set password minimum length rules to ensure the use of strong passwords in attempts to protect against brute force attacks. The TOE also accepts passwords composed of a variety of characters to support complex password composition. During authentication, no indication is given of the characters composing the password.

Logical Boundary Rationale for Security Management (FMT)

Security Function	Description
Security Management (FMT)	The TOE provides secure administrative services for management of general TOE configuration and TOE security functionality. There are two types of administrative users within the system: Security Administrator and Auditor (read only). All of the management functions are restricted to Security Administrators. The TOE administration occurs through REST API. The TOE provides the ability to perform the following actions: • Administer the TOE locally and remotely • Configure the access banner • Configure the cryptographic services • Update the TOE and verify the updates using digital signature capability prior to installing those updates • Specify the time limits of session inactivity

Logical Boundary Rationale for Protection of the TSF (FPT)

Security Function	Description
Protection of the TSF (FPT)	The TOE implements a number of measures to protect the integrity of its security features: • The TOE protects CSPs, including stored passwords and cryptographic keys, so they are not directly viewable or accessible in plaintext. • The TOE ensures that reliable time information is available for log accountability. The time can be configured through the REST API. The TOE performs self-tests to detect internal failures and protect itself from malicious updates.

Logical Boundary Rationale for TOE Access (FTA)

Security Function	Description
TOE Access (FTA)	The TOE will display a customizable banner when an administrator initiates a session. The TOE also enforces an administrator-defined inactivity timeout after which any inactive session is automatically terminated. Once a session has been terminated, the TOE requires the user to re-authenticate.

Logical Boundary Rationale for Trusted Path/Channels (FTP)

Security Function	Description
Trusted Path/Channels (FTP)	The TOE establishes a trusted path between the Unified Appliance and the administrative REST API using TLS/HTTPS. The TOE establishes a secure connection using TLS for: • Sending syslog data to a log server.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The followings are assumptions made for this TOE are as defined in NDcPP v2.2e Section 4.2.

5.1.1 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 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.

5.1.2 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 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.

5.1.3 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 and PP-Modules for particular types of Network Devices (e.g., firewall).

5.1.4 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 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.

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).

5.1.5 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.

5.1.6 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.

5.1.7 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.

5.1.8 A.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only)

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.

5.1.9 A.VS_REGULAR_UPDATES (applies to vNDs only)

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.

5.1.10 A.VS_ISOLATON (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.

5.1.11 A.VS_CORRECT_CONFIGURATION (applies to vNDs only)

For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

5.2 Threats

The followings are threats for this TOE as defined in NDcPP v2.2e Section 4.1.

5.2.1 Communications with the Network Device

5.2.1.1 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.

5.2.1.2 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.

5.2.1.3 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.

5.2.1.4 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.

5.2.2 Valid Updates

5.2.2.1 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.

5.2.3 Audited Activity

5.2.3.1 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.

5.2.4 Administrator and Device Credentials and Data

5.2.4.1 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 includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.

5.2.4.2 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.

5.2.5 Device Failure

5.2.5.1 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 [NDcPP].
- 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 PP and applicable Technical Decisions. Any additional security related functional capabilities that may be included in the product were not covered by this evaluation.
- The ST explicitly identifies the following excluded features:

- Unified Appliance clustering is not restricted; however, it is not evaluated.
- Any integration and/or communication with authentication servers such as vIDM is not evaluated.
- The use of SNMPv3 for monitoring is not restricted; however, it is not evaluated.
- Synchronization with an external NTP server is not restricted; however, this functionality is not evaluated.
- The Log Insight interface (an alternative Audit Server) is not enabled by default and is not evaluated.
- CLI (using SSH communications) is not enabled by default and is not evaluated.
- The TOE's debug mode is not intended for normal use and is not evaluated.
- Public and Hybrid Cloud functionality is not enabled by default; and is not evaluated.
- Container functionality is not enabled by default; and is not evaluated.
- The intra-TOE TLS connection between the UA and the NSX-T Edge is not evaluated and an Edge platform residing on another ESXi is not evaluated.
- NSX-T Edge Data-plane Services (vSphere Distributed Switch (VDS)/NSX Virtual Distributed Switch(NVDS)) and NSX Agents are excluded from the TOE; and are not evaluated.
- vCenter Server

- Consumers need to pay specific attention to all the functionality and features that are explicitly excluded from the scope of the evaluation and are identified in Section 1.7 of the ST.

6 Documentation

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

- VMware NSX-T Data Center 3.1 Common Criteria Configuration Guidance, Version 3.1 dated June 2022 [AGD]

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated. . Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration consists of the hardware, software, and firmware described in this section when configured in accordance with the documentation identified in Section 6.

The exact tested configuration is explained in full detail in the Assurance Activity Report.

VMware NSX-T Data Center 3.1, the TOE, is network virtualization software that provides network functionality for ESXi hypervisors and the virtual machines running on those hypervisors. The TOE abstracts network functions, including bridging, switching, and routing to create a virtual network that can connect to the physical network.

The TOE satisfies Case 1 as depicted in NDcPP v2.2e. The TOE is represented by the vND alone.

The following figure shows the detailed TOE boundary of VMware NSX-T Data Center 3.1. The different subsystems and interfaces are described briefly below:

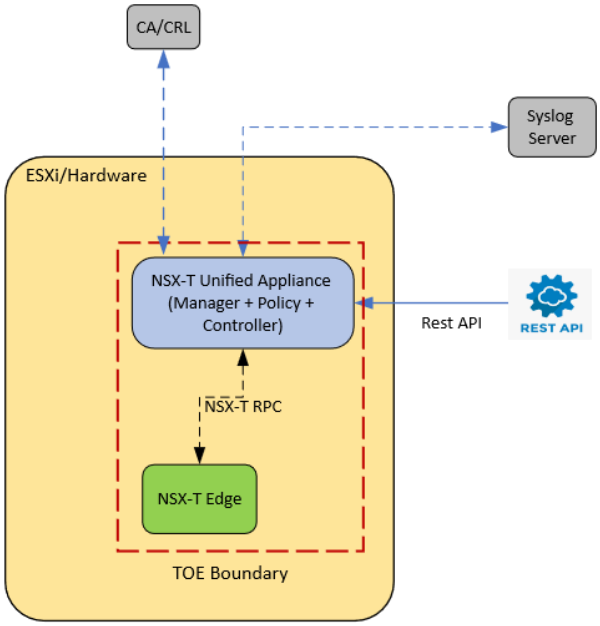

Figure 2 - TOE Physical Boundary

NSX-T Unified Appliance:

The NSX-T Unified Appliance contains a set of applications and daemons which implement the management functionality of NSX-T. Applications roles include Manager, Policy and Controller; and includes the HTTPS reverse proxy which serves as a TLS endpoint for the REST API. Policy controls the desired state configurations. Manager manages persistent data and communication between application roles; and communicates with Edge using TLS 1.1/1.2. Controller translates desired state into realized state and communicates with NSX-T Edge using TLS 1.1/1.2.

NSX Unified Appliance (Manager + Policy + Controller) is installed as a Virtual Machine (VM) on the ESXi hypervisor.

NSX-T Edge:

The NSX-T Edge Virtual Appliance contains a set of applications and daemons which bridge physical networking to the virtual network maintained by NSX-T.

Syslog Server:

The TOE establishes a trusted channel communication with the syslog server using TLS v1.1/1.2.

CA Server:

Server which contains the updated revocation list for the TOE.

REST API:

The main interface to NSX-T functionality is via a RESTful interface using HTTP over TLS 1.1/1.2. The REST API supports authentication using session-based authentication using a username and password. The API exposes interfaces to configure virtual networking constructs, and to observe the operational status of those constructs. Additionally, the API allows you to observe the operational status of the physical underlay network elements.

7.1.1 Non-TOE Hardware/Software/Firmware

The following components are not within the TOE Boundary and are located in the TOE environment:

- Syslog (Audit) Server (rsyslogd 8.20 was used in the evaluated configuration)
- VMware ESXi 6.7
- NSX Agent software (installed on the ESXi hypervisor)
- NSX and vSphere Distributed Switches (NVDS/VDS)
- Certificate Authority Server (CA) (XCA 2.1.0 was used in the evaluated configuration)

.

8 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 the VMware NSX-T Data Center 3.1, 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. The Independent Testing activity, Test Configurations and associated Test Tools are documented in the AAR sections 3, 4, 5 and 7, which is publicly available, and 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 and as summarized in the Assurance Activity Report for VMware NSX-T Data Center 3.1. 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 5 and CEM version 3.1 rev 5. The evaluation determined the VMware NSX-T Data Center 3.1 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDcPP.

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 NSX-T Data Center 3.1 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 [NDcPP].

The validators 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 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. 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 validators 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 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 NDcPP related to the examination of the information contained in the operational guidance documents.

The validators 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 found that the TOE was identified. Additionally, the team verified that both the TOE and its supporting documentation are consistently reference the same version and use the same nomenclature. The evaluation team also verified that the vendor website identified the TOE version accurately.

The validators 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 ran the set of tests specified by the Assurance Activities in the NDcPP and recorded the results in a Test Report, summarized in the ETR and AAR.

The validators 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 that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The following sources of public vulnerability information were searched:

- https://nvd.nist.gov/vuln/search
- https://cve.mitre.org/

The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on April 27 and June 30, 2022.

- VMware NSX-T
- VMware NSX-T Data Center 3.1
- VMware NSX Unified Appliance
- network virtualization platform
- NSX-T REST API
- Ubuntu 18.04
- Intel Xeon Gold 6230R
- Intel Xeon Gold 6230R (Cascade Lake)
- TLS 1.1

- TLS 1.2
- VMware BC-FJA
- Bouncy Castle FIPS Java API
- VMware’s OpenSSL FIPS Object module

The validators 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 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 NDcPP, 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 evaluated configuration instructions in the Configuration for Common Criteria Guide.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. The excluded functionality is specified in section 5.3 of this report. All other items and scope issues have been sufficiently addressed elsewhere in this document.

Additional functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

VMware NSX-T Data Center 3.1 Security Target, Version 1.6, July 12,2022 [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:

- Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
- Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
- Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
- Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
- collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]
- VMware NSX-T Data Center 3.1 Security Target [ST]
- VMware NSX-T Data Center 3.1 Common Criteria Guidance Addendum [AGD]
- Assurance Activity Report for VMware NSX-T Data Center 3.1 [AAR]