National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Citrix ADC Platinum Edition Version 11.1

Report Number:	**CCEVS-VR-10974-2019**
Dated:	**10/18/19**
Version:	**0.1**

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

Meredith Hennan

Jerome Myers

The Aerospace Corporation

Common Criteria Testing Laboratory

Danielle F Canoles

Thibaut Marconnet

Kenji Yoshino

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 Citrix ADC Platinum Edition Version 11.1 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 September 2019. 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 collaborative Protection Profile for Network Devices (NDcPP) + Errata 20180314 version 2.0e (NDcPPv2.0e).

The following table identifies the Technical Decisions associated with the collaborative Protection Profile for Network Devices at time of evaluation, whether they are applicable to the TOE in the evaluated configuration, and rationale for exclusion, if warranted:

Table 1 Technical Decisions

Identifier	Applicable	Exclusion Rationale (if applicable)
0425 – NIT Technical Decision for Cut-and-paste Error for Guidance AA	Yes	
0423 – NIT Technical Decision for Clarification about application of Rfl#201726rev2	Yes	
0412 – NIT Technical Decision for FCS_SSHS_EXT.1.5 SFR and AA discrepancy	Yes	
0411 – NIT Technical Decision for FCS_SSHC_EXT.1.5, Test 1 - Server and client side seem to be confused	No	This TD addresses SSH Client functionality. The TOE does not support SSH Client functionality.
0410 – NIT technical decision for Redundant assurance activities associated with FAU_GEN.1	Yes	
0409 – NIT decision for Applicability of FIA_AFL.1 to key-based SSH authentication	Yes	

0408 – NIT Technical Decision for local vs. remote administrator accounts	Yes	
0407 – NIT Technical Decision for handling Certification of Cloud Deployments	Yes	
0402 – NIT Technical Decision for RSA-based FCS_CKM.2 Selection	Yes	
0401 – NIT Technical Decision for Reliance on external servers to meet SFRs	Yes	
0400 – NIT Technical Decision for FCS_CKM.2 and elliptic curve-based key establishment	Yes	
0399 – NIT Technical Decision for Manual installation of CRL (FIA_X509_EXT.2)	Yes	
0398 – NIT Technical Decision for FCS_SSH*EXT.1.1 RFCs for AES-CTR	Yes	
0397 – NIT Technical Decision for Fixing AES-CTR Mode Tests	Yes	
0396 – NIT Technical Decision for FCS_TLSC_EXT.1.1, Test 2	Yes	
0395 – NIT Technical Decision for Different Handling of TLS1.1 and TLS1.2	No	This TD addresses TLS Server functionality. The TOE does not support TLS Server functionality.
0394 – NIT Technical Decision for Audit of Management Activities related to Cryptographic Keys	Yes	
0343 – NIT Technical Decision for Updating FCS_IPSEC_EXT.1.14 Tests	No	This TD addresses IPsec functionality. The TOE does not support IPsec.
0342 – NIT Technical Decision for TLS and DTLS Server Tests	No	This TD addresses (D)TLS Server functionality. The TOE does not support (D)TLS Server functionality.
0341 – NIT Technical Decision for TLS wildcard checking	Yes	
0340 – NIT Technical Decision for Handling of the basicConstraints extension in CA and leaf certificates	Yes	
0339 – NIT Technical Decision for Making password-based authentication optional in FCS_SSHS_EXT.1.2	Yes	
0338 – NIT Technical Decision for Access Banner Verification	Yes	
0337 – NIT Technical Decision for Selections in FCS_SSH*_EXT.1.6	Yes	
0336 – NIT Technical Decision for Audit requirements for FCS_SSH*_EXT.1.8	Yes	
0335 – NIT Technical Decision for FCS_DTLS Mandatory Cipher Suites	No	This TD addresses DTLS functionality. The TOE does not support DTLS.
0334 – NIT Technical Decision for Testing SSH when password-based authentication is not supported	No	This TD addresses SSH client functionality. The TOE does not claim FCS_SSHC_EXT.1.
0333 – NIT Technical Decision for Applicability of FIA_X509_EXT.3	Yes	

0324 – NIT Technical Decision for Correction of section numbers in SD Table 1	Yes	
0323 – NIT Technical Decision for DTLS server testing - Empty Certificate Authorities list	No	This TD addresses DTLS functionality. The TOE does not support DTLS.
0322 – NIT Technical Decision for TLS server testing - Empty Certificate Authorities list	No	This TD is associated with FCS_TLSS_EXT.2. The TOE does not include FCS_TLSS_EXT.2 functionality.
0321 – Protection of NTP communications	No	The TOE does not support an NTP server for automatic time updates.
0291 – NIT technical decision for DH14 and FCS_CKM.1	Yes	
0290 – NIT technical decision for physical interruption of trusted path/channel.	Yes	
0289 – NIT technical decision for FCS_TLSC_EXT.x.1 Test 5e	Yes	
0281 – NIT Technical Decision for Testing both thresholds for SSH rekey	Yes	
0262 – NIT Technical Decision for TLS server testing - Empty Certificate Authorities list	No	This TD has been archived
0260 – NIT Technical Decision for Typo in FCS_SSHS_EXT.1.4	No	This TD has been archived.
0259 – NIT Technical Decision for Support for X509 ssh rsa authentication IAW RFC 6187	Yes	
0257 – NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4	Yes	
0256 – NIT Technical Decision for Handling of TLS connections with and without mutual authentication	No	This TD is associated with FCS_DTLSC_EXT.2/FCS_TLSC_EXT.2. The TOE does not include this functionality.
0228 – NIT Technical Decision for CA certificates - basicConstraints validation	Yes	

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 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.

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.
- 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 2 Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Citrix ADC Platinum Edition Version 11.1
Protection Profile	collaborative Protection Profile for Network Devices (NDcPP) + Errata 20180314 version 2.0e (NDcPPv2.0e)
Security Target	Citrix ADC Platinum Edition Version 11.1 Security Target v1.2
Evaluation Technical Report	Citrix ADC Platinum Edition Version 11.1 ETR v1.3 Common Criteria NDcPP Assurance Activity Report for Citrix ADC Platinum Edition Version 11.1 Version 1.2
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Citrix Systems, Inc.
Developer	Citrix Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd Rockville, MD 20850

CCEVS Validators	Meredith Hennan Jerome Myers

3 Architectural Information

The Citrix ADC (formerly NetScaler) is an Application Delivery Controller that accelerates application performance, enhances application availability with advanced Layer 4 – Layer 7 load balancing, secures applications from attacks, and lowers server expenses by offloading computationally intensive tasks. The TOE comprises Citrix ADC running on the following hardware appliances.

- MPX 14030 FIPS
- MPX 14060 FIPS
- MPX 14080 FIPS

Citrix MPX 14XXX FIPS appliances are network devices that combine Layer 4 - Layer 7 load balancing and content switching with application acceleration, data compression, static and dynamic content caching, SSL acceleration, network optimization, application performance monitoring, application visibility, and robust application security via an application firewall. The ADC appliance supports NIST-approved FIPS 140-2 algorithms.

4 Security Policy

Security Audit

The TOE keeps local and remote audit records of security relevant events.

Cryptographic Support

The TOE provides cryptographic support for the SSH and TLS protocols. The related FIPS 140-2 validation details are provided in Table 3.

Table 3 CAVP Algorithm Testing References

Algorithm	CAVP Cert #	Standard	Operation	SFR
NITROXIII CNN3560-NFBE-G Algorithms (CMVP Cert. #2850)				
RSA	1634	FIPS 186-4	Signature Verification	FCS_COP.1/SigGen
DRBG	680	SP 800-90A	Random Bit Generation	FCS_RBG_EXT.1
AES	2034 3205	AES specified in ISO 18033-3 CBC specified in ISO 10116	TLS Encryption/Decryption DRBG Primitive	FCS_COP.1/DataEncryption
SHA	1780	ISO/IEC 10118-3:2004	Hashing	FCS_COP.1/Hash
HMAC	1233	ISO/IEC 9797-2:2011	Keyed-Hashing	FCS_COP.1/KeyedHash
Citrix FIPS Cryptographic Module Algorithms (CMVP Cert. #2988)				
RSA	2379	FIPS 186-4	Key Generation Signature Generation/Verification	FCS_CKM.1 FCS_COP.1/SigGen
ECDSA	1056	FIPS 186-4	Key Generation	FCS_CKM.1
DRBG	1417	SP 800-90A	Random Bit Generation	FCS_RBG_EXT.1
SHA	3626	ISO/IEC 10118-3:2004	Hashing	FCS_COP.1/Hash

Algorithm	CAVP Cert #	Standard	Operation	SFR
HMAC	2923	ISO/IEC 9797-2:2011	Keyed-Hashing	FCS_COP.1/KeyedHash
AES	4397	AES specified in ISO 18033-3 CBC specified in ISO 10116 CTR specified in ISO 10116	SSH Encryption/ Decryption DRBG Primitive	FCS_COP.1/DataEncryption
CVL (SP800-56A)	1106	SP 800-56A	Key Establishment	FCS_CKM.2

Identification and Authentication

The TOE provides two types of authentication to provide a trusted means for Security Administrators and remote endpoints to interact: X.509v3 certificate-based authentication for remote devices and password-based or public-key authentication for Security Administrators. Device-level authentication allows the TOE to establish a secure communication channel with a remote endpoint.

Security Administrators can set a minimum length for passwords (between 4 and 127 characters). Additionally, the TOE detects and tracks consecutive unsuccessful remote authentication attempts and will prevent the offending attempts from authenticating when a Security Administrator defined threshold is reached.

Security management

The TOE enables secure local and remote management of its security functions, including:

- Local console CLI administration
- Remote CLI administration via SSHv2
- Administrator authentication using a local database
- Timed user lockout after multiple failed authentication attempts
- Password complexity enforcement
- Role Based Access Control - the TOE supports several types of administrative user roles. Collectively these sub-roles comprise the “Security Administrator”
- Configurable banners to be displayed at login
- Timeouts to terminate administrative sessions after a set period of inactivity
- Protection of secret keys and passwords

Protection of the TSF

The TOE ensures the authenticity and integrity of software updates through hash comparison and requires administrative intervention prior to the software updates being installed.

TOE Access

Prior to login, the TOE displays a banner with a message configurable by the Security Administrator. The TOE terminates user connections after an Authorized Administrator configurable amount of time.

Trusted Path/Channels

The TOE uses TLS to provide a trusted channel between itself and remote syslog and LDAP servers.

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

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.

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 [NDcPPv2.0e] will not include any requirements on physical tamper protection or other physical attack mitigations. The [NDcPPv2.0e] 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.

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).

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 NDcPPv2.0e. It is assumed that this protection will be covered by cPPs 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 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.

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.

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.

5.2 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.

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.

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 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 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. Please see Section 7.2 of this report for further information on the specific functionality and features that are excluded from the scope of this evaluation.

6 Documentation

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

- Citrix ADC Platinum Edition Version 11.1 Security Target v1.2 [ST]
- Common Criteria Evaluated Configuration Guide for ADC 11.1 Platinum Edition v1.1 [CCECG]
- Citrix ADC MPX, September 16, 2019
- NetScaler 11.1, September 13, 2019

The [CCECG] includes all required information for configuring the TOE into the evaluated configuration. The Citrix ADC MPX and NetScaler 11.1 guides are general user guides which may be used to configure any excluded functionality with the exception of (see Section 7.2 for additional details):

- IPv6
- NTP based updates to the time
- Use of superuser privileges except as described in [CCECG]
- ADC GUI (HTTP/HTTPS), ADC Nitro API and ADM

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

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE evaluated configuration consists of one of the MPX series appliances listed in Section 3 above when configured in accordance with the documentation identified in Section 6. The TOE also supports (sometimes optionally) secure connectivity with several other IT environment devices as described in Table 4 below,

Table 4 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with an SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
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. The syslog server must support communications using TLS 1.1 or TLS 1.2.
LDAP Server	Yes	The LDAP server is used for authentication of administrator credentials The LDAP server must support communications using TLS 1.1 or TLS 1.2.

The following figure provides a visual depiction of an example of a typical TOE deployment. The TOE boundary is surrounded with **hashed red lines**.

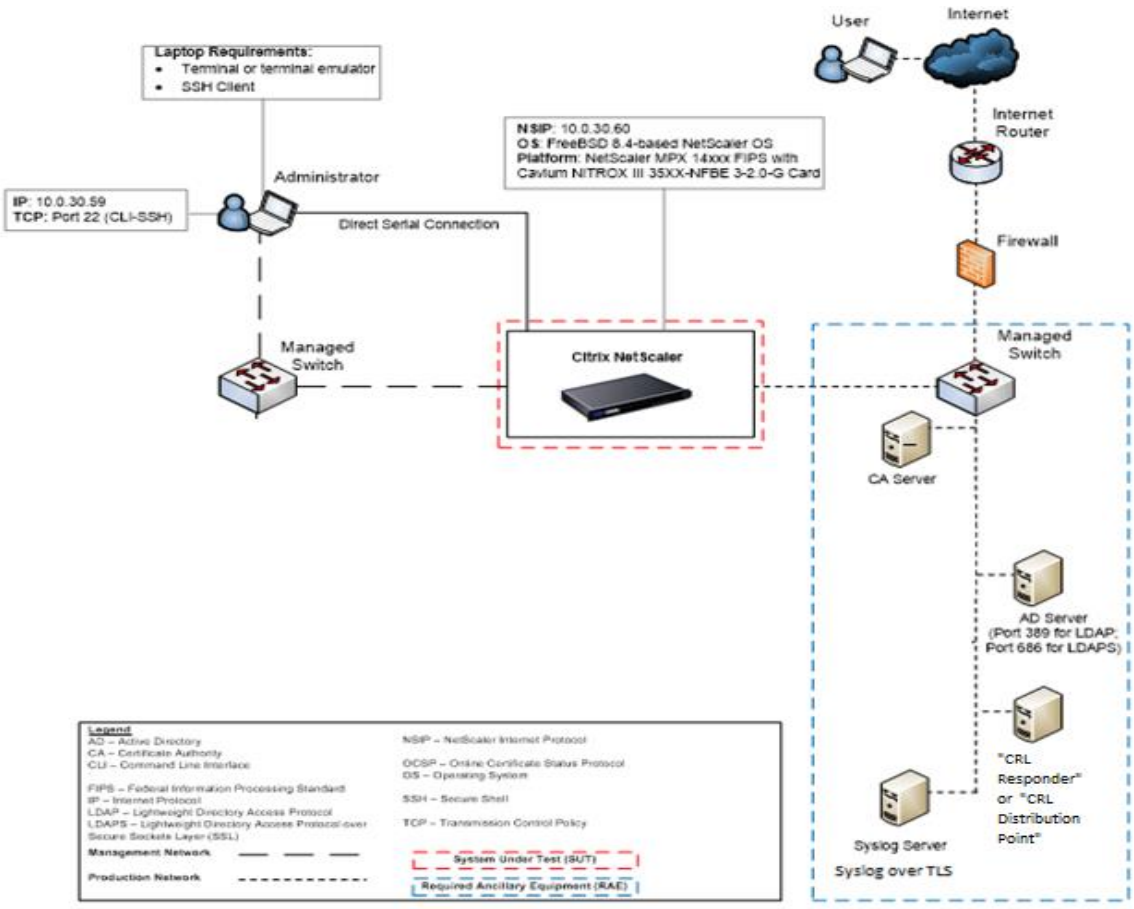

Figure 1 Deployment Configuration of TOE

7.1.1 Physical Boundaries

The TOE is a hardware and software solution that is comprised of the security appliance models described above in section 1.3. The TOE guidance documentation can be found at http://docs.citrix.com/en-us/netscaler/11-1.html# but the product needs to be administered in accordance with the [CCESG] as described in Section 6 of this document to ensure proper operation within the evaluated configuration.

7.2 Excluded Functionality

Hardware and software located in the TOE environment are not included in the scope of the evaluation.

Only security functionality specified in the SFRs and TSS is covered by the scope of evaluation. The following other product features or functionality are considered unevaluated, because they are not included in the scope of the Security Target:

- Web Logging
- Application Firewall
- Global Server Load Balancing (GSLB)
- AAA-TM Authentication
- External authentication methods: Kerberos, TACACS+, SAML, RADIUS
- Responder
- Rewrite (URL Transformation)
- Layer 3 Routing
- Vpath
- RISE
- High Availability
- CloudBridge
- CallHome
- Integrated Disk Caching
- General TLS VPN functionality
- Clientless VPN functionality
- SSL acceleration – SSL termination for application servers[1]
- AppFlow
- AppQoE
- BGP
- Cache Redirection
- Compression Control
- Content Accelerator
- Content Filtering
- Content Switching
- FEO
- OSPF
- LSN
- RDP Proxy
- RIP
- HTM Injection
- Http DoS Protection
- Integrated Caching
- Surge Protection
- ISIS
- Priority Queuing
- Reputation
- Sure Connect
- NetScaler Push

[1] TLS used by the TSF is in scope and evaluated by FCS_TLSC_EXT.1.

Additionally, the following features may not be used when the TOE is operated in a manner compliant with this Security Target:

- IPv6
- NTP based updates to the time
- Use of superuser privileges except as described in [CCECG]
- ADC GUI (HTTP/HTTPS), ADC Nitro API and ADM

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary Evaluation Test Report for Citrix ADC Platinum Edition Version 11.1, which is not publicly available. The Assurance Activities Report posted on the NIAP PCL provides a non-proprietary 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 the vendor-provided guidance documentation and ran the tests specified in the NDcPPv2.0e. The Independent Testing activity is documented in Sections 4 and 5 of the Assurance Activities Report, which is publicly available, and is not duplicated here. The configuration of the TOE, configuration of the test environment, and test tools utilized are documented in Section 3 of the Assurance Activities Report.

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 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 the Citrix ADC Platinum Edition Version 11.1 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDcPPv2.0e.

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 Citrix ADC Platinum Edition Version 11.1 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 NDcPPv2.0e.

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 Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the NDcPPv2.0e 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 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 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 NDcPPv2.0e and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

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 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 on October 10, 2019. The details of the vulnerability search can be found in Section 5.15.1 of the AAR.

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 NDcPPv2.0e, 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 NDcPPv2.0e, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validators have no supplemental comments. All validator comments are adequately covered in other sections of this document.

11 Annexes

Not applicable.

12 Security Target

Citrix ADC Platinum Edition Version 11.1 Security Target v1.2

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 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. collaborative Protection Profile for Network Devices (NDcPP) + Errata 20180314 version 2.0e (NDcPPv2.0e)
6. Citrix ADC (formerly NetScaler) Platinum Edition Version 11.1 Common Criteria Security Target, Version 1.2, September 2019
7. Common Criteria NDcPP Assurance Activity Report for Citrix ADC Platinum Edition Version 11.1, Version 1.3, October 2019
8. Citrix ADC Platinum Edition Version 11.1 Evaluation Technical Report, Version 1.3, September 2019