122

CERTIFICATION REPORT No. CRP294

Citrix NetScaler Platinum Edition Load Balancer
Version 10.5
running on MPX 9700-FIPS, MPX 10500-FIPS, MPX 12500-FIPS, MPX 15500-FIPS appliances

Issue 1.0

November 2015

CESG Certification Body
IA Service Management, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme ('the Scheme') and has met the specified Common Criteria (CC) [CC] requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this Certification Report.			
Sponsor	Citrix Systems Inc.	Developer	Citrix Systems Inc.
Product(s), Version(s)	Citrix NetScaler Platinum Edition Load Balancer Version 10.5		
Platform(s)	MPX 9700-FIPS, MPX 10500-FIPS, MPX 12500-FIPS, MPX 15500-FIPS appliances		
Description	The NetScaler Platinum Edition Load Balancer Version 10.5 is an application performance accelerator incorporating a Secure Sockets Layer (SSL/TLS) Virtual Private Network (VPN).		
CC Version	Version 3.1 Release 4		
CC Part 2	Extended	CC Part 3	Conformant
PP(S) Conformance	Protection Profile for Network Devices v1.1 [PP], with Errata #3 [PP_ERR3] applied		
EAL or [c]PP	Assurance Package as defined in [PP]		
CLEF	CGI		
CC Certificate	P294	Date Certified	13th November 2015

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation (TOE) in meeting its Security Target (ST) [ST], which prospective consumers are advised to read. To ensure that the ST gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against that baseline. Both parts of the evaluation were performed in accordance with [PP], [PP_ERR3], CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issuing of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (CCRA)

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this Certification Report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

SENIOR OFFICIALS GROUP – INFORMATION SYSTEMS SECURITY (SOGIS) MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (MRA)

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to the above Agreement [MRA] and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

CCRA logo **CC logo** **SOGIS MRA logo**

[1] All judgements contained in this Certification Report are covered by the CCRA [CCRA] and the SOGIS MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of NetScaler Platinum Edition Load Balancer Version 10.5 to the Sponsor, Citrix Systems Inc., as summarised on page 2 'Certification Statement' of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers of NetScaler Platinum Edition Load Balancer Version 10.5 should understand the specific scope of the certification by reading this report in conjunction with the Security Target (ST) [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation, in accordance with the assurance activities defined in the Protection Profile (PP) for Network Devices [PP], on 5th November 2015:

- **NetScaler Platinum Edition Load Balancer Version 10.5 running on MPX 9700 FIPS, MPX 10500 FIPS, MPX 12500 FIPS, MPX 15500 FIPS appliances.**

The Developer was Citrix Systems Inc.

4. The evaluated configuration of the product is described in this report as the 'Target of Evaluation' (TOE).

5. The TOE is an application performance accelerator incorporating a Secure Sockets Layer (SSL/TLS) Virtual Private Network (VPN). The scope of this evaluation includes the TOE when operating as a dedicated self-contained appliance (i.e. running on dedicated hardware supplied as part of the TOE).

6. The TOE type is a "network device" in the sense of [PP]. All MPX-FIPS appliances provide a serial port to connect a console directly to the appliance for management, and a Liquid Crystal Display (LCD) on the front of each appliance displays real-time statistics, diagnostics and alerts. All platforms include a FIPS 140-2 Level 3 validated crypto card and FIPS 140-2 Level 1 validated version of OpenSSL.

7. Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' of this report. The physical scope of the TOE is the appliance, and the logical scope of the TOE is as defined in [PP]. The components of the product that are not included in the evaluation are defined in [ST] Section 1.3.3.

8. An overview of the TOE and its product architecture are provided in Chapter IV 'Product Architecture' of this report. Configuration requirements are specified in [ST] Section 1.2.1.

Protection Profile Conformance

9. The TOE is certified as achieving conformance to the following PP:

- **Protection Profile for Network Devices [PP], with Errata #3 [PP_ERR3] applied.**

[ST] claims "exact" conformance to [PP], as required by that PP.

Security Target

10. [ST] fully specifies the TOE's Security Objectives, the Threats and Organisational Security Policies (OSPs) which these Objectives counter/meet, and the Security Functional Requirements (SFRs) that elaborate the Objectives. Some of the SFRs are taken from CC Part 2 [CC2] and the extended SFRs are taken from [PP]; use of that standard facilitates comparison with other evaluated products.

11. The TOE security policies are detailed in [ST]. The OSPs that must be met are specified in [ST] Section 3.2.

12. The environmental assumptions related to the operating environment are detailed in Chapter III (in 'Environmental Requirements') of this report.

Evaluation Conduct

13. The CESG Certification Body monitored the evaluation, which was performed by the CGI Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in [ST]. The results of that work, completed in November 2015, were reported in the Evaluation Technical Report (ETR) [ETR].

Evaluated Configuration

14. The TOE should be used in accordance with the environmental assumptions specified in [ST]. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

15. The TOE should be used in accordance with its supporting guidance documentation included in the evaluated configuration, as detailed in [ECG].

Conclusions

16. The conclusions of the CESG Certification Body are summarised on page 2 'Certification Statement' of this report.

Recommendations

17. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure delivery, receipt, installation, configuration and operation of the TOE.

Disclaimers

18. This Certification Report and associated Certificate applies only to the specific version of the product in its evaluated configuration (i.e. the TOE). This is specified in Chapter III 'Evaluated Configuration' of this report. The ETR [ETR] on which this Certification Report is based relates only to the specific items tested.

19. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability that exploitable vulnerabilities may be discovered after the Evaluators' penetration tests were completed. This report reflects the CESG Certification Body's view on that date (see paragraph 46).

20. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the date of the penetration tests (as detailed in Chapter V) and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

21. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE but should only be applied in accordance with a consumer's risk management policy. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

22. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

23. Note that the opinions and interpretations stated in this report in the section 'Recommendations' above, and in Chapter II 'TOE Security Guidance', are based on the experience of the CESG Certification Body in performing similar work under the Scheme.

II. TOE SECURITY GUIDANCE

Introduction

24. The following sections provide guidance of particular relevance to consumers of the TOE.

Delivery and Installation

25. On receipt of the TOE, the consumer should check that the evaluated version has been supplied and should check that the security of the TOE has not been compromised during delivery. Specific advice on delivery and installation is provided in the TOE documents below:

- [ECG] Chapter 3, subsection "Verifying the Hardware";
- [ECG] Chapter 3, subsection "Upgrading the NetScaler Software Version".

Guidance Documents

26. Specific configuration advice is provided in the Secure Configuration document below:

- [ECG].

27. [ECG] refers to standard documentation, for the product, that is provided in the bundle of documents for download at:

https://www.citrix.com/content/dam/citrix/en_us/documents/downloads/netscaler-adc/Common-criteria-documents-for-NetScaler-10.5.zip.

28. To maintain secure operation, the consumer should use administrative accounts assigned to the sysadmin command policy for the majority of network related day-to-day activities, while assigning superuser command policies to other authorised administrators to perform those activities that relate to the management of the appliance itself, as detailed in [ECG] Chapter 4, subsection "Recommended Appliance Management Use Cases".

III. EVALUATED CONFIGURATION

TOE Identification

29. The TOE is NetScaler Platinum Edition Load Balancer Version 10.5, which consists of the firmware 'build-10.5-53.22.nc' (which is downloaded in the file 'build-10.5-53.22_nc.tgz'), running on one of the following Citrix MPX-FIPS platforms:

- MPX 9700-FIPS;
- MPX 10500-FIPS;
- MPX 12500-FIPS;
- MPX 15500-FIPS.

TOE Documentation

30. The relevant guidance documents for the evaluated configuration are identified in Chapter II (in 'Guidance Documents') of this report.

31. All guidance relevant to the operation of the TOE in its evaluated configuration should be downloaded from:

https://www.citrix.com/content/dam/citrix/en_us/documents/downloads/netscaler-adc/Common-criteria-documents-for-NetScaler-10.5.zip

TOE Scope

32. The TOE Scope is defined in [ST] Sections 1.2 and 1.3. Functionality that is outside the TOE Scope is defined in [ST] Section 1.3.3. The TOE Scope is consistent with that defined in [PP], with the understanding of a "network device" in the sense of [PP] Section 1.1, i.e. "a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise".

TOE Configuration

33. The evaluated configuration of the TOE is defined in [ST] Sections 1.2.1 and 1.3, and depicted in Figure 1 below. Specific configuration advice is provided in [ECG].

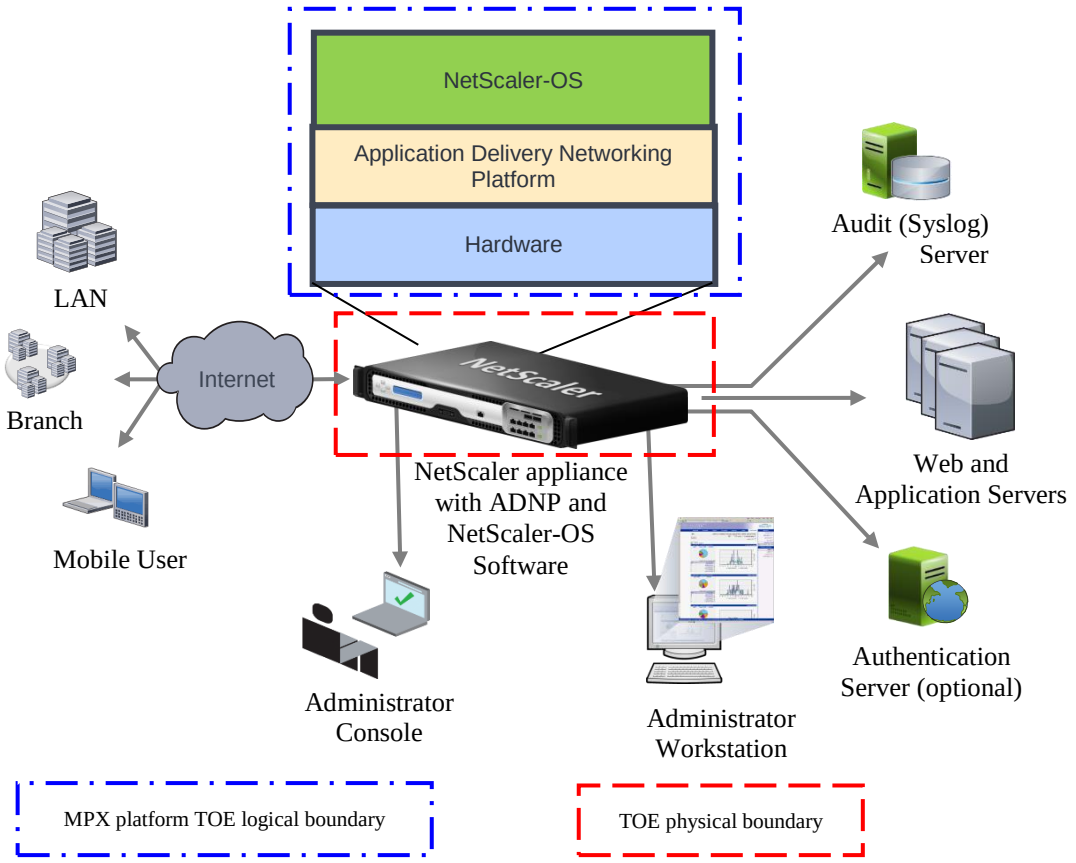

Figure 1 - TOE Configuration

Environmental Requirements

34. The environmental assumptions for the TOE are stated in [ST] Section 3.3.

35. The TOE was evaluated running on MPX 9700-FIPS, MPX 10500-FIPS, MPX 12500-FIPS and MPX 15500-FIPS appliances.

36. The environmental IT configuration is detailed in [ST] Section 1.2.6. The following hardware and software are part of the TOE environment:

- Administrator console and workstation for management of the TOE;
- Application server(s);
- Audit (Syslog) server;
- VPN client(s);
- Networks (including the Internet and the Enterprise Network);
- Authentication server (LDAP, RADIUS) (optional).

Test Configurations

37. The Evaluators used the test configuration depicted in Figure 2 below for their testing, and they performed their testing on each of the distinct hardware platforms in the section 'Environmental Requirements' above.

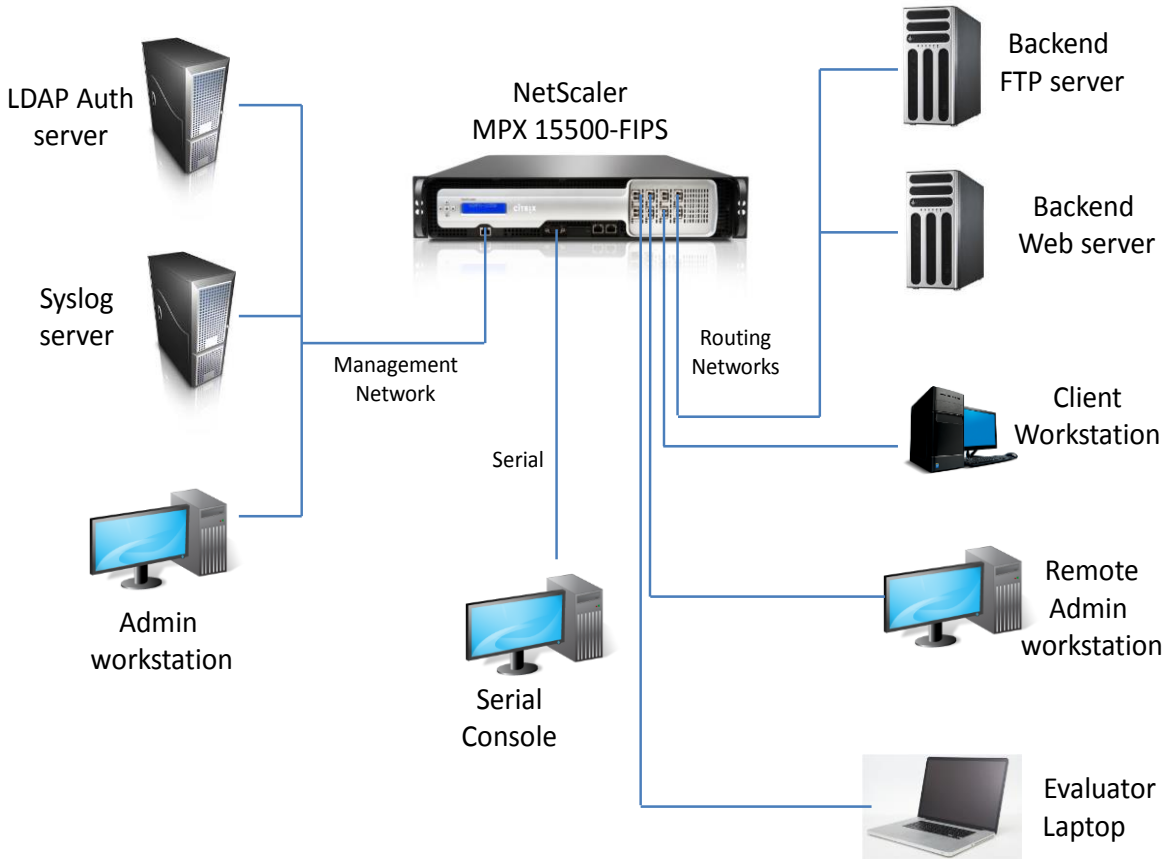

Figure 2 - Test Environment

38. The Evaluators performed an analysis of the platform variations between the appliance models being evaluated, from which they determined that it was sufficient to perform the testing on a single sample platform, as the platforms differ only in terms of throughput permitted by licensing. Citrix appliance model MPX 15500-FIPS was selected. One additional test was also performed on the low-end MPX 9700-FIPS platform to demonstrate the throttling applied to traffic throughput.

IV. PRODUCT ARCHITECTURE

Introduction

39. This Chapter gives an overview of the TOE's main architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration' of this report.

Product Description and Architecture

40. The TOE is composed of the NetScaler-OS, the Application Delivery Networking Platform, and the hardware appliance. Those logical components run directly on the NetScaler appliance hardware:

a) The 'Load Balancer' component manages the connections between clients and servers. Clients establish a connection with the NetScaler, rather than directly with a server. When the NetScaler receives an application request from a client, it establishes a connection with the appropriate application server. That allows the Load Balancer to sort and prioritize application requests from multiple clients and requires only a single connection on the application server to handle requests from multiple clients.

b) The 'Access Gateway' component provides a TLS VPN connection that is used as a tunnel to enable remote administrator connections to be made. In a deployment configuration, a remote administrator first opens a TLS VPN connection to the NetScaler appliance to a publicly accessible VPN vserver IP address. When connecting to the vserver, the administrator is authenticated as an authorised VPN user by means of the configured authentication mechanism. After successful authentication, a TLS tunnel is established through which the administrator can then address the NSIP and open an SSH connection to it in order to access the CLI for management operations;

c) The above components run on top of the Application Delivery Networking Platform (ADNP) on the appliances. The ADNP is the specialised kernel and packet-processing engine, which coordinates the operations of the other software components, and it controls the network interfaces, memory management, and system timing.

41. The NetScaler-OS incorporates a version of OpenSSL that is separately validated against FIPS 140-2 (certificate #1747). The hardware appliance integrates a version of the Cavium NITROX XL 1600-NFBE HSM Family card that is separately validated against FIPS 140-2 (certificate #2316).

TOE Dependencies

42. The TOE dependencies are identified in Chapter III 'Environmental Requirements' of this report.

V. TOE TESTING

Evaluator Testing

43. The Evaluators devised and ran a total of 50 independent security functional tests. No anomalies were found.

44. The Evaluators also devised and ran a total of 4 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

45. All but one of the Evaluators tests were performed on the MPX 15500-FIPS. The remaining (throttling) test was performed on the MPX 9700-FIPS, as discussed in Chapter III (in 'Test Configurations') of this report.

46. The Evaluators completed their penetration tests on 2nd October 2015.

Vulnerability Analysis

47. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables.

Platform Issues

48. The Citrix NetScaler platforms, which are included within the scope of the TOE, are listed in Chapter III (in 'TOE Identification') of this report. No platform-related issues were identified.

VI. REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation (comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1, Introduction and General Model, Common Criteria Maintenance Board, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2, Security Functional Components, Common Criteria Maintenance Board, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3, Security Assurance Components, Common Criteria Maintenance Board, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, Participants in the Arrangement Group, 2nd July 2014

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[ECG] Common Criteria Evaluated Configuration Guide for NetScaler 10 Platinum Edition, Citrix Systems, Document code: October 13, 2015 17:56:12 Version 3.6.

[ETR] Evaluation Technical Report, CGI CLEF, LFL/T279/ETR, Issue 1.1, 5th November 2015.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Management Committee, Senior Officials Group – Information Systems Security (SOGIS), Version 3.0, 8th January 2010.

[PP] Protection Profile for Network Devices, Information Assurance Directorate, Version 1.1, 8 June 2012.

[PP_ERR3] Security Requirements for Network Devices,
Information Assurance Directorate,
Errata #3, dated 3rd November 2014.

[ST] Common Criteria Security Target for NetScaler Platinum Edition Load Balancer,
Version 10.5,
Citrix Systems,
CN12-ST-0001, Issue 1.0, 13 October 2015.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.8, August 2013.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.5, August 2013.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.5, August 2013.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 3.1, August 2013.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML); standard CC abbreviations (e.g. TOE, TSF) in CC Part 1 [CC1]; and UK Scheme abbreviations and acronyms (e.g. CLEF, CR) in [UKSP00].

ADNP	Application Delivery Networking Platform
CLI	Command Line Interface
FIPS	Federal Information Processing Standard
IP	Internet Protocol
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
MRA	Mutual Recognition Agreement
NSIP	The IP address of the NetScaler appliance itself
RADIUS	Remote Authentication Dial-In User Service
SSH	Secure Shell
SOGIS	Senior Officials Group - Information Systems Security
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual Private Network

VII. CERTIFICATE

The final two pages of this document contain the Certificate (front and back) for the TOE.

CESG Certified Product

Common Criteria

P294

This is to certify that

Citrix NetScaler Platinum Edition Load Balancer

Version 10.5

running on MPX 9700-FIPS, MPX 10500-FIPS, MPX 12500-FIPS, MPX 15500-FIPS

has been evaluated under the terms of the

Common Criteria Scheme

and complies with the requirements of

Protection Profile for Network Devices v1.1, with Errata #3 applied

Common Criteria

UKAS PRODUCT CERTIFICATION 0122

SOGIS IT SECURITY CERTIFIED

AUTHORISED BY
DIRECTOR GENERAL
FOR CYBER SECURITY

THIS PRODUCT WAS EVALUATED BY
CGI

DATE AWARDED
13th November 2015

UKAS PRODUCT CERTIFICATION
0122

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is accredited by the United Kingdom Accreditation Service (UKAS) to *ISO/IEC17065:2012* to provide product conformity certification as follows:

Category: Type Testing Product Certification of IT Products and Systems.
Standards: Common Criteria for Information Technology Security Evaluation (CC) EAL1 – EAL7.

Details are provided on the UKAS website (www.ukas.org).

The IT Product identified in this certificate has been evaluated at an accredited and licensed/approved Evaluation Facility or at an Evaluation Facility established under the laws, statutory instruments, or other official administrative procedures of the United Kingdom using the Common Methodology for IT Security Evaluation, version 3.1 and CC Supporting Documents as listed in the Certification/Validation Report for conformance to the Common Criteria for IT Security Evaluation, version 3.1. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification/Validation Report. The Evaluation has been conducted in accordance with the provisions of the Common Criteria Scheme and the conclusions of the Evaluation Facility in the Evaluation Technical Report are consistent with the evidence adduced. This certificate is not an endorsement of the IT Product by CESG or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by CESG or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

All judgements in this certificate, and in the associated Certification Report, are covered by the Arrangement.

Senior Officials Group – Information Systems Security (SOGIS)
Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOGIS MRA), Version 3.0

The CESG Certification Body is a Participant to the above Agreement. The current Participants to the above Agreement are detailed on the SOGIS Portal (www.sogisportal.eu). The mark (left) confirms that this conformant certificate has been authorised by a Participant to the above Agreement and it is the Participant's statement that this certificate has been issued in accordance with the terms of the above Agreement. The judgements contained in this certificate and in the associated Certification Report are those of the compliant Certification Body which issues them and of the Evaluation Facility which performed the evaluation. Use of the mark does not imply acceptance by other Participants of liability in respect of those judgements or for loss sustained as a result of reliance upon those judgements by a third party.

All judgements in this certificate, and in the associated Certification Report, are covered by the Agreement.

In conformance with the requirements of *ISO/IEC17065:2012*, the CCRA and the SOGIS MRA, the CESG Certification Body's website (www.cesg.gov.uk) provides additional information as follows:

- Type of product (i.e. product category); and
- Details of product manufacturer (i.e. as appropriate: vendor/developer name, postal address, website, point of contact, telephone number, fax number, email address).