122

CERTIFICATION REPORT No. CRP274

Citrix NetScaler Platinum Edition Load Balancer Version 10.0

running on
specified MPX hardware platforms and
specified VPX virtualized platforms

Issue 1.0

July 2013

CESG Certification Body
AAS Delivery Office, 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 and Version:	Citrix NetScaler Platinum Edition Load Balancer Version 10.0		
Platform:	*Hardware Platforms:* MPX 5550, MPX 5650, MPX 5750, MPX 8200, MPX 8400, MPX 8600, MPX 8800, MPX 9700 FIPS, MPX 10500, MPX 10500 FIPS, MPX 11500, MPX 12500, MPX 12500 FIPS, MPX 13500, MPX 14500, MPX 15500, MPX 15500 FIPS, MPX 16500, MPX 17500, MPX 17550, MPX 18500, MPX 19500, MPX 19550, MPX 20500, MPX 20550, MPX 21500 and MPX 21550; *XenServer 6.0.2 Virtualised Platforms:* VPX 10, VPX 200, VPX 1000 and VPX 3000.		
Description:	The NetScaler Platinum Edition Load Balancer Version 10.0 is a dedicated application performance accelerator incorporating a Secure Sockets Layer (SSL) Virtual Private Network (VPN) with policy-based access control and a Web Application Firewall.		
CC Version:	Version 3.1 release 3		
CC Part 2:	Conformant	CC Part 3:	Conformant
EAL:	EAL2 augmented by ALC_FLR.2		
PP Conformance:	None		
CLEF:	SiVenture		
CC Certificate:	P274	Date Certified:	17 July 2013

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 CC Parts 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 MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Citrix NetScaler Platinum Edition Load Balancer Version 10.0 (Build 74.4.nc)[2] 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 Version 10.0 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation to CC EAL2 augmented by ALC_FLR.2 on 8 July 2013:

- **Citrix NetScaler Platinum Edition Load Balancer Version 10.0 running on specified MPX hardware platforms and specified VPX virtualised platforms (as stated on page 2).**

4. The Developer was Citrix Systems Inc.

5. The NetScaler Version 10.0 appliance (i.e. the TOE on one of the MPX or VPX platforms) incorporates three software components that work together to provide secure access to web-based applications, such as Citrix XenDesktop or XenApp, from an external network. The three software components are the Load Balancer, Access Gateway, and the Web Application Firewall. These run on top of the Application Delivery Networking Platform on either a dedicated MPX hardware platform (the specific platforms within the scope of this evaluation are listed in [ST] Section 1.2.6) or within a virtual machine managed by XenServer running on generic server hardware (the specific platforms within the scope of this evaluation are listed in [ST] Section 1.2.7). Further details are provided in [ST] Section 1.2.

6. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III (in 'Evaluated Configuration') of this report.

7. TOE administrators can access the TOE through a direct serial connection, which gives them access to the Command Line Interface (CLI).

8. The use of authentication servers and a syslog server are optional but, if used, they form part of the TOE environment.

[2] Hereinafter referred to as 'NetScaler Version 10.0' or 'the TOE'.

9. It should be noted that use of Layer 3 routing and management, using the NetScaler GUI Dashboard Command Center application and NetScaler XML-API interface, is excluded from the scope of the evaluation. A complete list of features excluded from the scope of evaluation is provided in the Security Target [ST]. Details of evaluated configuration requirements are provided in the Evaluated Configuration Guide [ECG].

10. An overview of the TOE and its product architecture can be found in Chapter IV (in 'Product Architecture') of this report. Configuration requirements are specified in Section 1 of [ST].

Security Target

11. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats which these Objectives counter and the Security Functional Requirements (SFRs) and Security Functionality that elaborate the Objectives. All of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

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

Evaluation Conduct

13. The TOE's SFRs and the security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from that of Citrix NetScaler Platinum Edition Load Balancer Version 9.3, which had previously been certified [CR] by the UK IT Security Evaluation and Certification Scheme to the CC EAL2 assurance level (augmented with ALC_FLR.2). For the evaluation of Citrix NetScaler Platinum Edition Load Balancer Version 10.0, the Evaluators reused the previous evaluation results where appropriate.

14. The CESG Certification Body monitored the evaluation, which was performed by the SiVenture Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed on 8 July 2013, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

15. The TOE should be used in accordance with the environmental assumptions specified in the Security Target [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.

16. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Conclusions

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

Recommendations

18. 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.

19. In addition, the Evaluators' comments and recommendations are as follows:

a) TOE consumers should browse to the https://www.citrix.com/ website to initiate a download of [ECG], rather than clicking on any URL link to the Citrix website that they receive, in order to ensure that they are not being redirected to a website that is masquerading as the Citrix site.

b) The TOE administrator's attention is drawn to the guidance in [ECG] Section 4 regarding the truncation of signature file when bound to an AppFW policy.

20. The TOE relies on the underlying platform, Citrix XenServer 6.0.2, for the virtualised platforms (VPX 10, VPX 200, VPX 1000 and VPX 3000). System integrators and risk owners using the TOE should therefore make suitable arrangements to satisfy themselves that they have appropriate confidence in the guest domain separation mechanisms of that underlying platform.

Disclaimers

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

22. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This report reflects the CESG Certification Body's view at the time of certification.

23. 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.

24. 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.

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

26. Note that the opinions and interpretations stated in this report under 'Recommendations' and '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

27. The following sections provide guidance of particular relevance to purchasers of the TOE.

Delivery and Installation

28. On receipt of the TOE, the consumer should check that the evaluated versions of its constituent components have been supplied, and 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 detailed below:

a) Section 3 of Evaluated Configuration Guide [ECG], which should be downloaded from the *Security & Compliance* > *Common Criteria* option from the left hand menu of the https://www.citrix.com/support.html website.

b) Section 2 of Migration Guide [MG].

29. In particular, Users should note that the integrity of the downloaded firmware packages can be verified using the checksums:

a) Hardware Appliance Firmware (provided in file "build-10.0-74.4_nc.tgz") MD5 checksum = de0ff39959440be032336eefbb50f884.

b) Virtual Appliance Firmware (provided in file "NSVPX-XEN-10.0-71.4_nc.xva") MD5 checksum = 843EEC7A67377453F9F81F769AE42BC9.

30. The MPX platforms are shipped directly from Citrix Systems Inc. to TOE consumers, using a reputable carrier. Prior to shipment, Citrix attaches a shipping label identifying the exact product name, product part number, product serial number, and customer name to the outside of the shipping box. Citrix notifies the consumer of the tracking number, which can be used to track the shipment during delivery. Upon receipt, the consumer should verify that the delivery matches the details of the order placed and should verify that the listed serial number matches the actual serial number of the enclosed product. The consumer should also examine the MPX platform to verify that the tamper seals are not damaged.

Guidance Documentation

31. Specific configuration advice is provided in the Secure Configuration documentation detailed below:

- Evaluated Configuration Guide [ECG];
- Migration Guide [MG];
- VPX Getting Started Guide [VPX].

32. The Administration Guide documentation is as follows:

- Administration Guide [AG];
- Application Firewall Guide [AFG];
- Application Security Guide [ASG];
- Command Reference Guide [CRG];
- Networking Guide [NG];
- Policy Configuration and Reference Guide [PG];
- Traffic Management Guide [TMG].

III. EVALUATED CONFIGURATION

TOE Identification

33. The TOE is Citrix NetScaler Platinum Edition Load Balancer Version 10.0, which consists of one of the following:

a) The firmware NetScaler 10.0 Build 74.4.nc' (which is downloaded in the file 'build-10.0-74.4_nc.tgz') running on one of the Citrix MPX hardware platforms described on page 2.

b) The firmware 'NetScaler 10.0 Build 74.4.nc' (which is downloaded in the file 'NSVPX-XEN-10.0-71.4_nc.xva') running on one of the XenServer 6.0.2[3] VPX virtualised platforms described on page 2.

TOE Documentation

34. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in 'Guidance Documentation') of this report.

35. With the exception of [ECG], the relevant guidance documentation should be downloaded in the same manner as the firmware image, linked on the same webpage, as identified in Chapter II (in 'Delivery and Installation') of this report.

36. The Evaluated Configuration Guide [ECG] should be downloaded from the public area of the Citrix website, and should be accessed in accordance with the recommendation provided in Chapter I (in 'Recommendations') of this report.

TOE Scope

37. The TOE Scope is defined in the Security Target [ST] Sections 1.3 and 1.4. Functionality that is outside the TOE Scope is defined in [ST] Section 1.4.3 and is summarised as follows:

- Content Switching;
- Content Rewrite;
- Caching;
- Compression;
- Web Logging;
- Layer 3 Routing[4];

[3] The appropriate patches should be applied to XenServer 6.0.2, including (but not limited to) XS602ECC001, XS602ECC002, XS602ECC003, XS602ECC004 and XS602ECC005.

- Load Balancing between NetScaler appliances;
- NetScaler GUI Dashboard Command Center application and NetScaler XML-API interface[5].

TOE Configuration

38. The evaluated configuration of the TOE is defined in [ST] Section 1.3 and specific configuration advice is provided in [ECG].

39. The TOE configuration is shown in Figure 1 below.

[4] Layer 3 routing (L3 mode) is out of scope as this enables IP forwarding, allowing traffic to be routed according to static routes in the routing table, rather than being routed via the virtual servers in accordance with the configured policies.

[5] These are alternative methods of managing NetScaler. However, only the CLI method of management is included in the evaluated configuration.

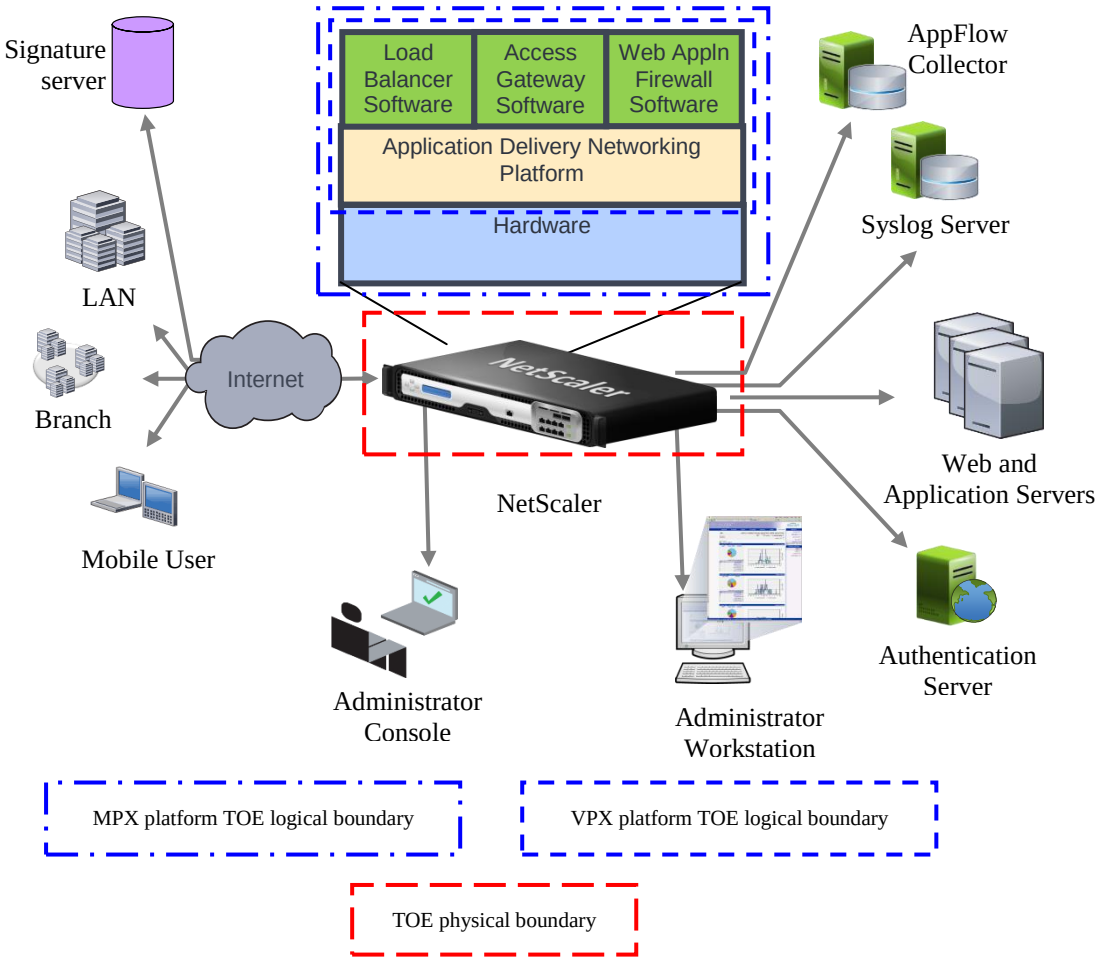

Figure 1 TOE Configuration

Environmental Requirements

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

41. The TOE was evaluated running on Citrix MPX hardware platforms and XenServer 6.0.2 VPX virtualised platforms as stated on page 2.

42. The environmental IT configuration is detailed in [ST] section 1.3.4.

Test Configurations

43. The Developer used configurations consistent with that depicted in Figure 1 above for their testing, and they performed their testing on each of the distinct platforms in the section 'Environmental Requirements' above.

44. The Evaluators performed an analysis of the platform variations between the platform models being evaluated, from which they determined that it was sufficient to perform the testing on two sample platforms. Citrix platform models MPX 15500-FIPS and MPX 8200 were

selected. The Evaluators also completed an installation of the virtual platform VPX 3000. Those test platforms were agreed in advance with the CESG Certification Body. The test configuration used by the Evaluators was consistent with that depicted in Figure 1 above.

45. The VPX 3000 was tested on a Citrix XenServer 6.0.2 platform with the patches XS602ECC001, XS602ECC002, XS602ECC003 and XS602ECC004 applied[6].

46. The evaluator testing in the Lab was performed using the test configuration shown in Figure 2.

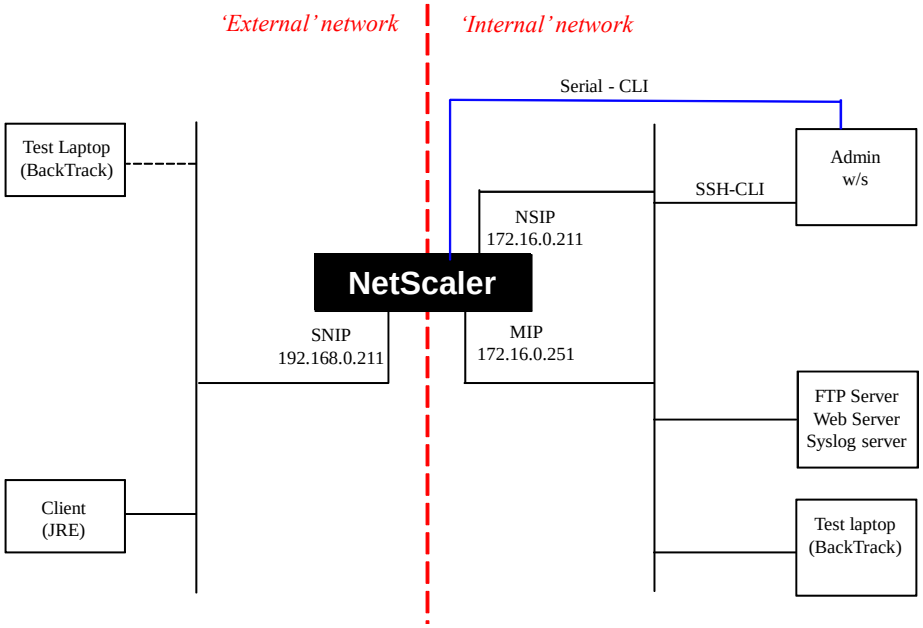

Figure 2 Evaluator test configuration

[6] This reflects the patches available at the time of evaluator testing. The patch XS602ECC005 was released after evaluator testing.

IV. PRODUCT ARCHITECTURE

Introduction

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

Product Description and Architecture

48. The architecture of the TOE incorporates three software components that work together to provide secure access to web-based applications. The three software components are as follows:

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.

b) The 'Access Gateway' component is an SSL VPN which provides policy-based access control for network resources. The Access Gateway allows administrators to control access based on the identity of the user that is connecting and the device that user is connecting from.

c) The 'Web Application Firewall' component provides firewall protection against attacks at the Application Layer of the Open Systems Interconnection (OSI) Basic Reference Model. Traffic which matches a pre-defined signature will be treated as defined in the signature (this may be any combination of blocking, logging, and maintaining statistics for matches).

49. The above three components run on top of the Application Delivery Networking Platform (ADNP) on the platforms. 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.

TOE Design Subsystems

50. The high-level TOE subsystems, and their security features/functionality, are as follows:

- *Kernel Subsystem*: coordinates the other subsystems and provides kernel level services;
- *Authentication Subsystem*: authenticates administrators and VPN users;
- *Logging Subsystem*: accepts and stores audit events;
- *SSL VPN Subsystem*: facilitates file-server access and provides access to other file services, such as print services;

- *Application Firewall (AppFW) Learning Subsystem*: provides dynamic data firewalling functionality to protect internal networks from attack;
- *Application Firewall (AppFW) Signature Subsystem*: manages signatures that are used in AppFW for Signature based protections;
- *NSDynamic Routing Subsystem*: stores and processes routing information for routing protocols, such as RIP, BGP, and OSPF;
- *NS CRL Subsystem*: maintains and updates Certificate Revocation Lists (CRLs);
- *Access Control Subsystem*: controls the actions of administrators. All management functions must pass through the Access Control Subsystem, which has the ability to stop unauthorized or unsafe actions;
- *Management Subsystem*: provides the administrator interfaces and translates administrator commands;
- *Hard Disk Drive (HDD) Subsystem*: provides persistent storage for statistics, audit data, and application firewall data;
- *Flash Memory Subsystem*: provides storage for the configuration file and SSL certificate keys.

51. Figure 3 below shows the high-level design subsystems, and their internal and external interfaces.

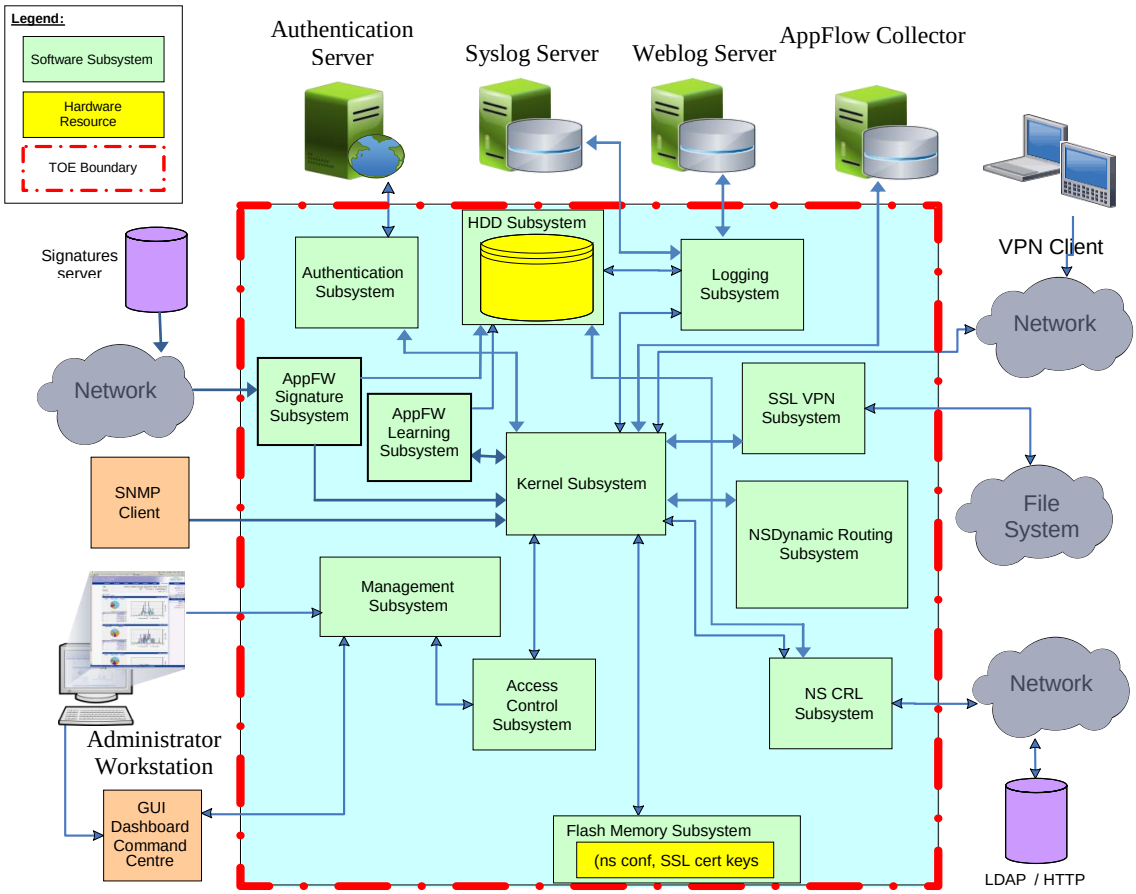

Figure 3 TOE Subsystems and Interfaces

TOE Dependencies

52. The TOE dependencies are identified in Chapter III (in 'Environmental Requirements') of this report.

TOE Interfaces

53. The external TOE Security Functionality Interfaces (TSFI), as shown in Figure 3 above, are described as follows:

- *Network Interface*: used as the connection point for VPN clients and general network traffic (e.g. LDAP/HTTP CRL repository);
- *Authentication Interface*: used for connection to authentication servers;
- *External Logging Interface*: used for connection to external weblog servers (use of which is excluded from evaluated configuration) and external syslog servers;

- *File Services Interface*: used for connection to backend (Samba) servers;
- *Command Line Interface (*SSH, *Telnet*[7]*)*: used for management;
- *SNMP Interface*: used to provide status information to monitoring IP devices on the network.

54. The external interfaces of the TOE shown in Figure 2 above, which are not available in the evaluated configuration, are:

- *GUI Dashboard Command Centre Interface*: used for management;
- *Apache Interface*: used for management (using XML-API or CLI over the Administrator Workstation connection to the Management Subsystem).

[7] The use of Telnet should include adequate protection of the connection, in accordance with A.NetCon in [ST].

V. TOE TESTING

Developer Testing

55. The Developer's security tests covered:

- all SFRs;
- all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems') of this report;
- all Security Functions (SFs);
- the TSFI, as identified in Chapter IV (in 'TOE Interfaces') of this report.

56. The majority of MPX models share hardware with other MPX models; the only distinction between the models being the available throughput, which is controlled by licensing. The grouping of distinct physical hardware (i.e. the same hardware can be used to install each model listed in the group) is as follows:

- MPX 5550, MPX 5650, MPX 5750
- MPX 8200, MPX 8400, MPX 8600, MPX 8800
- MPX 10500, MPX 12500, MPX 15500
- MPX 17500, MPX 19500, MPX 21500
- MPX 9700 FIPS, MPX 10500 FIPS, MPX 12500 FIPS, MPX 15500 FIPS
- MPX 11500, MPX 13500, MPX 14500, MPX 16500, MPX 18500, MPX 20500
- MPX 17550, MPX 19550, MPX 20550, MPX 21550

57. The Developer's tests were performed on each distinct physical hardware platform and also on the VPX 3000 virtualised platform.

58. The Evaluators witnessed a sample of the Developer's security tests.

Evaluator Testing

59. The Evaluators devised and ran a total of 11 independent security functional tests, different from those performed by the Developer. No anomalies were found.

60. The Evaluators also devised and ran a total of 9 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

61. The Evaluators completed their penetration tests on 24 May 2013.

Vulnerability Analysis

62. 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

63. 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 issues were identified.

VI. REFERENCES

[AFG] Citrix Application Firewall Guide Citrix® NetScaler® 10,
Citrix Systems Inc.,
Document code: July 10 2012 01:39:48.

[AG] Citrix NetScaler Administration Guide Citrix® NetScaler® 10,
Citrix Systems Inc.,
Document code: August 22 2012 03:58:42.

[ASG] Citrix Application Security Guide Citrix® NetScaler® 10,
Citrix Systems Inc.,
Document code: July 10 2012 01:42:00.

[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-2009-07-001, Version 3.1 R3, July 2009.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Components,
Common Criteria Maintenance Board,
CCMB-2009-07-002, Version 3.1 R3, July 2009.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Components,
Common Criteria Maintenance Board,
CCMB-2009-07-003, Version 3.1 R3, July 2009.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Participants in the Arrangement Group,
May 2000.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2009-07-004, Version 3.1 R3, July 2009.

[CR] Common Criteria Certification Report No. CRP267,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, March 2012.

[CRG] Citrix NetScaler Command Reference Guide Citrix® NetScaler® 10,
Citrix Systems Inc.,
Document code: June 19 2012 01:15:06.

[ECG] Common Criteria Evaluated Configuration Guide for Citrix® NetScaler® 10,
Citrix Systems Inc.,
Document code: May 13, 2013 17:56:12.

[ETR] Citrix NetScaler Platinum Edition Load Balancer Version 10.0 Evaluation Technical Report,
SiVenture CLEF,
CN10-TR-0001, Version 1-1, 08 July 2013.

[MG] Citrix NetScaler Migration Guide Citrix® NetScaler® 10,
Citrix Systems Inc.,
Document code: August 23 2012 05:55:31.

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

[NG] Citrix NetScaler Networking Guide Citrix® NetScaler® 10,
Citrix Systems Inc.,
Document code: May 17 2012 05:06:06.

[PG] Citrix NetScaler Policy Configuration and Reference Guide Citrix® NetScaler® 10,
Citrix Systems Inc.,
Document code: May 17 2012 06:29:23.

[ST] Common Criteria Security Target for NetScaler Platinum Edition Load Balancer Version 10.0,
Citrix Systems Inc.,
CN10-ST-0001, Issue 1-1, 05 July 2013.

[TMG] Citrix NetScaler Traffic Management Guide Citrix® NetScaler® 10,
Citrix Systems Inc.,
Document code: October 9 2012 01:22:00.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.6, December 2009.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.3, December 2009.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.3, October 2010.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.4, December 2009.

[VPX] Citrix NetScaler VPX Getting Started Guide Citrix® NetScaler® 10,
Citrix Systems Inc.,
Document code: May 18 2012 03:01:29.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML); standard Common Criteria 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
API	Application Programming Interface
AppFW	Application Firewall
BGP	Border Gateway Protocol
CLI	Command Line Interface
CRL	Certificate Revocation List
FIPS	Federal Information Processing Standard
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5 (a one-way hash function)
MIP	Mapped IP (address)
MPX	NetScaler Physical Hardware Platform
NS	NetScaler (platform)
NSIP	NetScaler IP (address)
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
SNIP	SubNet IP (address)
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
VPN	Virtual Private Network
VPX	NetScaler Virtual Platform
w/s	Workstation
XML	Extensible Markup Language

VIII. CERTIFICATE

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

CESG CERTIFICATION BODY

CERTIFICATE No.
P274

This Certificate confirms that

Citrix NetScaler Platinum Edition Load Balancer, Version 10.0

running on MPX 5550, MPX 5650, MPX 5750, MPX 8200, MPX 8400, MPX 8600, MPX 8800, MPX 10500, MPX 12500, MPX 15500, MPX 17500, MPX 19500, MPX 21500, MPX 9700 FIPS, MPX 10500 FIPS, MPX 12500 FIPS, MPX 15500 FIPS, MPX 11500, MPX 13500, MPX 14500, MPX 16500, MPX 18500, MPX 20500, MPX 17550, MPX 19550, MPX 20550, MPX 21550, VPX 10, VPX 200, VPX 1000 and VPX 3000

has been evaluated under the terms of the

UK IT Security Evaluation and Certification Scheme

and complies with the requirements for

EAL2 augmented by ALC_FLR.2

COMMON CRITERIA (ISO 15408) ASSURANCE LEVEL

The scope of the evaluated functionality was as claimed by the Security Target and as confirmed by the associated Certification Report **CRP274**.

Certification is not a guarantee of freedom from security vulnerabilities. This certificate reflects the CESG Certification Body's view at the time of certification. It is the responsibility of users (existing and prospective) to check whether any security vulnerabilities have been discovered since the date of the Evaluators' final penetration tests.

AUTHORISATION
Director for Information Assurance

DATE
17 July 2013

122

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is accredited by the United Kingdom Accreditation Service (UKAS) to ***EN 45011:1998 (ISO/IEC Guide 65:1996)*** 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; and
- Information Technology Security Evaluation Criteria (ITSEC) E1 - E6.

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

Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA), May 2000

The CESG Certification Body is a Participant to the above Arrangement. The current Participants to the above Arrangement are detailed on the Common Criteria Portal (www.commoncriteriaportal.org). The mark (left) confirms that this Common Criteria certificate has been authorised by a Participant to the above Arrangement and it is the Participant's statement that this certificate has been issued in accordance with the terms of the above Arrangement. Upon receipt of this Common Criteria certificate, the vendor(s) may use the mark in conjunction with advertising, marketing and sales of the IT product for which this certificate is issued.

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 judgments contained in this certificate and in the associated Certification Report are those of the compliant Certification Body which issued 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 judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

The IT product identified in this certificate has been evaluated by the SiVenture Commercial Evaluation Facility (an accredited and approved Evaluation Facility of the UK) using the ***Common Methodology for Information Technology Security Evaluation***, ***Version 3.1***, for conformance to the ***Common Criteria for Information Technology Security Evaluation, Version 3.1***. This certificate applies only to the specific version and release of the IT product in its evaluated configuration and in conjunction with the complete, associated Certification Report. The evaluation has been conducted in accordance with the provisions of the UK IT Security Evaluation and Certification 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.

In conformance with the requirements of ***EN 45011:1998 (ISO/IEC Guide 65:1996)***, 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).