122

CERTIFICATION REPORT No. CRP267

Citrix NetScaler Platinum Edition Load Balancer
Version 9.3

running on MPX 9700-FIPS, MPX 10500-FIPS, MPX 12500-FIPS, MPX 15500-FIPS, MPX 5500, MPX 7500, MPX 9500, MPX 10500, MPX 11500, MPX 12500, MPX 13500, MPX 14500, MPX 15500, MPX 16500, MPX 17500, MPX 17550, MPX 18500, MPX 19500, MPX 19550, MPX 20500, MPX 20550, MPX 21500, MPX 21550, VPX 10, VPX 200, VPX 1000, VPX 3000

Issue 1.0

March 2012

CESG Certification Body
IACS 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 and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.

Sponsor:	Citrix Systems Inc.	Developer:	Citrix Systems Inc.
Product and Version:	Citrix NetScaler Platinum Edition Load Balancer Version 9.3		
Platform:	MPX 9700-FIPS, MPX 10500-FIPS, MPX 12500-FIPS, MPX 15500-FIPS, MPX 5500, MPX 7500, MPX 9500, MPX 10500, MPX 11500, MPX 12500, MPX 13500, MPX 14500, MPX 15500, MPX 16500, MPX 17500, MPX 17550, MPX 18500, MPX 19500, MPX 19550, MPX 20500, MPX 20550, MPX 21500, MPX 21550, VPX 10, VPX 200, VPX 1000, VPX 3000		
Description:	The NetScaler Platinum Edition Load Balancer Version 9.3 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:	P267	Date Certified:	12 March 2012

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

The issue 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**

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 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.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to this Agreement 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 carried out 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 9.3 (Build 53.5.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 are advised to read 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 21 February 2012:

- **Citrix NetScaler Platinum Edition Load Balancer Version 9.3 (Build 53.5.nc)** running on MPX 9700-FIPS, MPX 10500-FIPS, MPX 12500-FIPS, MPX 15500-FIPS, MPX 5500, MPX 7500, MPX 9500, MPX 10500, MPX 11500, MPX 12500, MPX 13500, MPX 14500, MPX 15500, MPX 16500, MPX 17500, MPX 17550, MPX 18500, MPX 19500, MPX 19550, MPX 20500, MPX 20550, MPX 21500, MPX 21550, VPX 10, VPX 200, VPX 1000, VPX 3000.

4. The Developer was Citrix Systems Inc.

5. 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 'Evaluated Configuration' of this report.

6. The NetScaler appliance (i.e. the TOE on one of the above platforms) incorporates three software components (i.e. 'the Load Balancer', the 'Access Gateway', and the 'Web Application Firewall') that work together to provide secure access to web-based applications from an external network.

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.

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

[2] Hereinafter referred to as 'NetScaler Version 9.3' or 'the TOE'.

provided in the Security Target [ST]. Details of evaluated configuration requirements are provided in the Evaluated Configuration Guide [CCECG].

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

Security Claims

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, remain mostly unchanged from that of Citrix NetScaler Platinum Edition Load Balancer Version 9.2, which has 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 9.3, the Evaluators made some reuse of 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 in February 2012, were reported in the Evaluation Technical Report [ETR].

Conclusions and Recommendations

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

16. Prospective consumers of Citrix NetScaler Platinum Edition Load Balancer Version 9.3 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. 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.

17. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure receipt, installation, configuration and operation of the TOE.

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

- TOE consumers should browse to the **https://www.citrix.com/** website to initiate download of [CCECG], 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;

- TOE consumers should adhere closely to the administrative guidance, especially that provided in [CCECG], in order to maintain and operate the product securely in accordance with the evaluated configuration.

Disclaimers

19. This report is only valid for the evaluated TOE. This is specified in Chapter III ‘Evaluated Configuration’ of this report.

20. 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.

21. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the ETR was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

22. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. 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.

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

II. TOE SECURITY GUIDANCE

Introduction

24. The following sections provide guidance that is of particular relevance to purchasers of the TOE.

Delivery

25. On receipt of the TOE, the consumer is recommended to check that the evaluated versions of its constituent components have been supplied, and to check that the security of the TOE has not been compromised during delivery.

26. The appliances 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 appliance to verify that the tamper seals are not damaged.

27. The consumer should follow the guidance in the Evaluated Configuration Guide [CCECG] (which should be downloaded from **https://www.citrix.com/**) to download the certified version of software via the Citrix support website (**http://support.citrix.com/**). The consumer is able to verify the integrity of the downloaded package by performing an MD5 hash of the software package and comparing it to the values in the checksum file relating to the software package posted on the secure area of the (**http://support.citrix.com/**) website; which is also provided in [CCECG] and is detailed below:

- Virtual Appliance: (provided in file "NSVPX-XEN-9.3-53.5_nc.xva") MD5 checksum = 7de2fd771e1a6d0d66627636bdbe15e3;

- Appliance Firmware: (provided in file "build-9.3-53.5_nc.tgz") MD5 checksum = 906f47b2faf614f9296cbae6a21439d3.

Installation and Guidance Documentation

28. The Installation and Secure Configuration documentation is as follows:

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

29. 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 [PCRG].

III. EVALUATED CONFIGURATION

TOE Identification

30. The TOE is NetScaler Platinum Edition Load Balancer Version 9.3, which consists of one of the following:

a. the software ‘build-9.3-53.5.nc’ (which is downloaded in the file ‘build-9.3-53.5_nc.tgz’), running on one of the following Citrix hardware platforms:

i. MPX 9700-FIPS;

ii. MPX 10500-FIPS;

iii. MPX 12500-FIPS;

iv. MPX 15500-FIPS;

v. MPX 5500;

vi. MPX 7500;

vii. MPX 9500;

viii. MPX 10500;

ix. MPX 11500;

x. MPX 12500;

xi. MPX 13500;

xii. MPX 14500;

xiii. MPX 15500;

xiv. MPX 16500;

xv. MPX 17500;

xvi. MPX 17550;

xvii. MPX 18500;

xviii. MPX 19500;

xix. MPX 19550;

xx. MPX 20500;

xxi. MPX 20550;

xxii. MPX 21500;

xxiii. MPX 21550;

b. the software ‘nsvpx-9.3-53.5.nc’ (which is downloaded in the file ‘NSVPX-XEN-9.3-53.5_nc.xva’), running on one of the following virtualised platforms:

i. VPX 10;

ii. VPX 200;

iii. VPX 1000;

iv. VPX 3000.

TOE Documentation

31. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in ‘Installation and Guidance Documentation’) of this report.

32. The relevant guidance documentation (except for the Evaluated Configuration Guide [CCECG]) is downloaded in the same manner as the firmware image, linked on the same webpage, as identified in Chapter II (in ‘Delivery’) of this report.

33. The Evaluated Configuration Guide [CCECG] is downloaded from the public area of the Citrix website, and should be accessed in accordance with the recommendation provided in Chapter I (in ‘Conclusions and Recommendations’) of this report.

TOE Scope

34. 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:

a. Content Switching;

b. Content Rewrite;

c. Caching;

d. Compression;

e. Web Logging;

f. Layer 3 Routing[3];

g. Load Balancing between NetScaler appliances;

h. NetScaler GUI Dashboard Command Center application and NetScaler XML-API interface[4].

TOE Configuration

35. The evaluated configuration of the TOE is defined in [ST] Section 1.3 and in the Evaluated Configuration Guide [CCECG], and is reproduced in Figure 1 below.

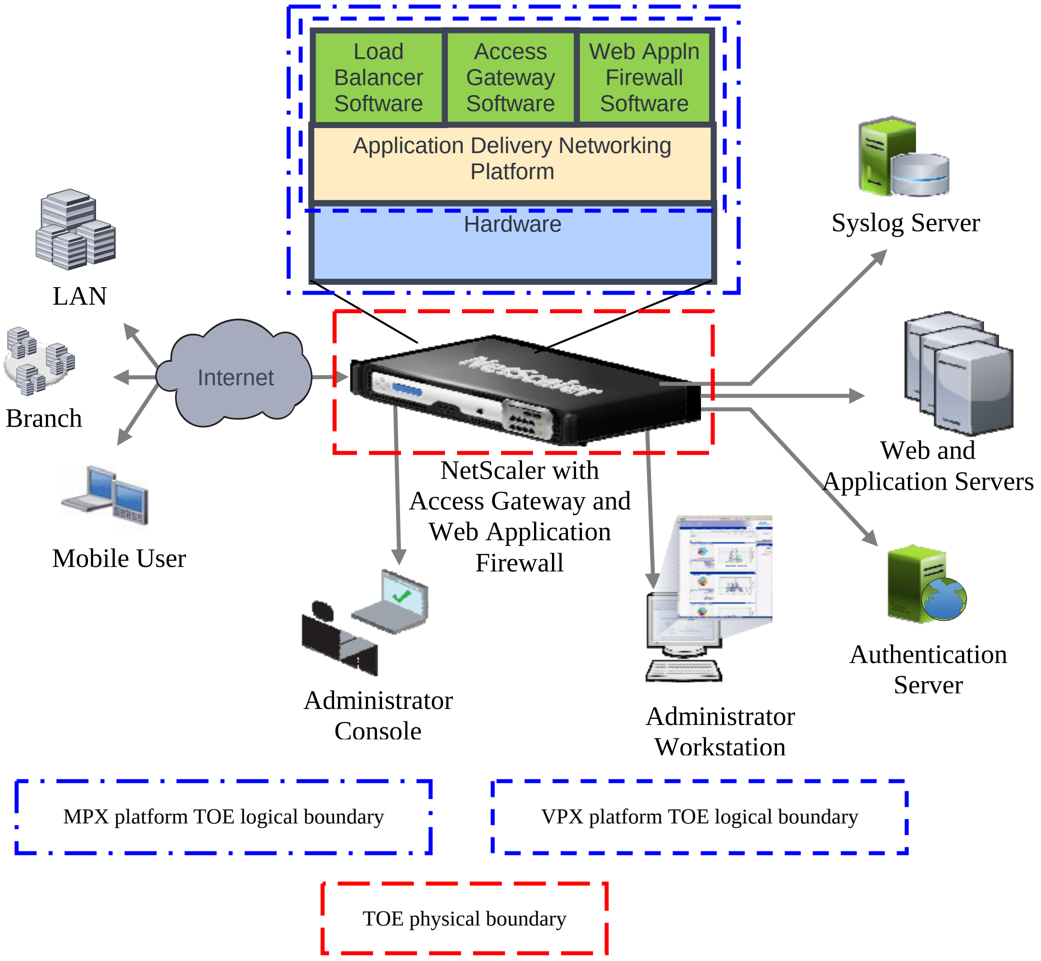
Load Balancer Software
Access Gateway Software
Web Appln Firewall Software
Application Delivery Networking Platform
Hardware
LAN
Branch
Internet
Mobile User
NetScaler with Access Gateway and Web Application Firewall
Syslog Server
Web and Application Servers
Authentication Server
Administrator Console
Administrator Workstation
MPX platform TOE logical boundary
VPX platform TOE logical boundary
TOE physical boundary

Figure 1 TOE Configuration

[3] 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.

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

Environmental Requirements

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

37. The TOE was evaluated running on Citrix hardware platforms MPX 9700-FIPS, MPX 10500-FIPS, MPX 12500-FIPS, MPX 15500-FIPS, MPX 5500, MPX 7500, MPX 9500, MPX 10500, MPX 11500, MPX 12500, MPX 13500, MPX 14500, MPX 15500, MPX 16500, MPX 17500, MPX 17550, MPX 18500, MPX 19500, MPX 19550, MPX 20500, MPX 20550, MPX 21500 and MPX 21550, and on virtualised platforms VPX 10, VPX 200, VPX 1000, VPX 3000.

38. The environmental IT configuration is detailed in [ST] Section 1.3.4.

Test Configuration

39. 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 hardware platforms in the section ‘Environmental Requirements’ above.

40. 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 two sample platforms. Citrix appliance models MPX 15500-FIPS and MPX 17500 were selected. The Evaluators also completed an installation of the virtual appliance VPX 1000. 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.

IV. PRODUCT ARCHITECTURE

Introduction

41. 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

42. 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:

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).

43. The above three 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.

TOE Design Subsystems

44. The 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.

45. Figure 2 below shows the high-level design subsystems, and their internal and external interfaces.

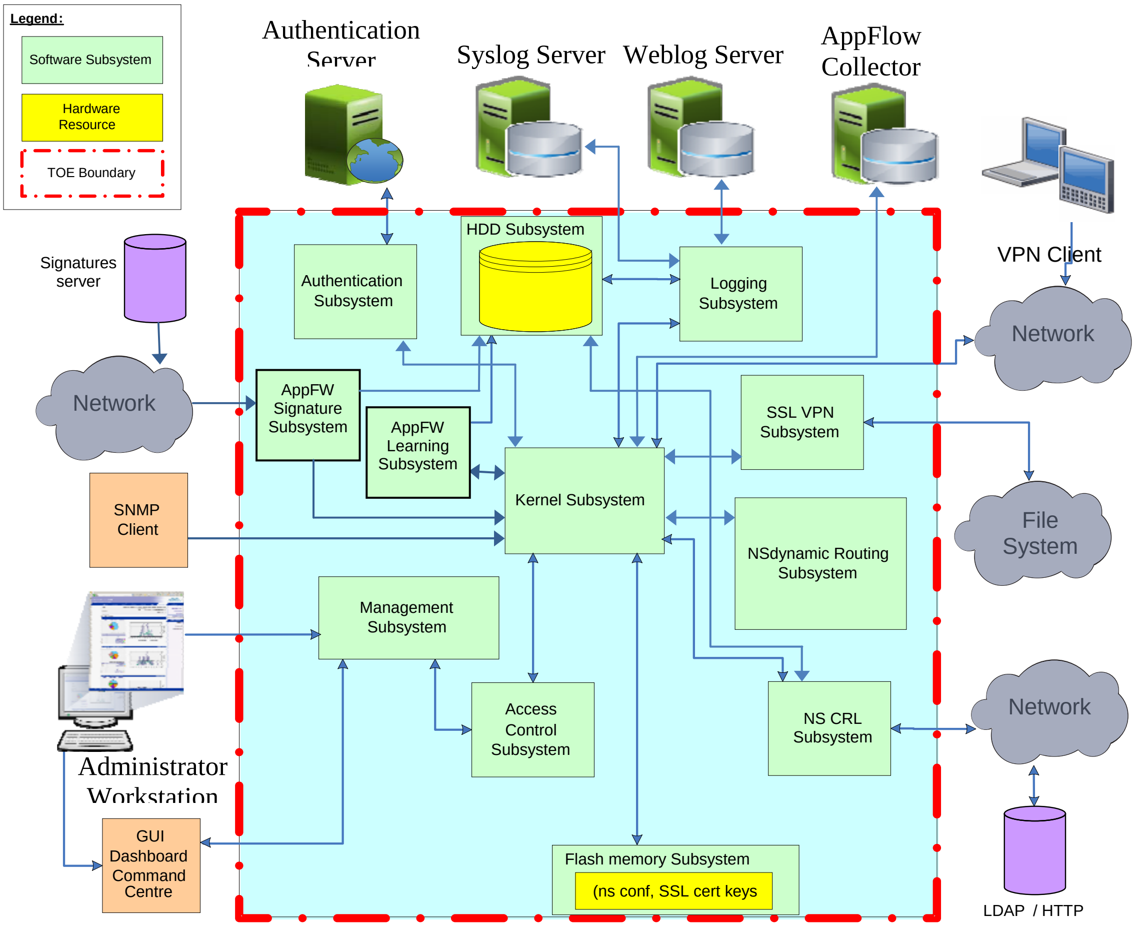

Figure 2 TOE Subsystems

TOE Dependencies

46. The TOE dependencies are identified in Chapter III (in ‘Environmental Requirements’) of this report.

TOE Interfaces

47. The external TOE Security Functions Interface (TSFI), as shown in Figure 2 above, is 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*[5]*)*: used for management;
- *SNMP Interface*: used to provide status information to monitoring IP devices on the network.

48. 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).

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

V. TOE TESTING

TOE Testing

49. The Developer’s 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.

50. 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 5500;
- MPX 7500, MPX 9500;
- 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.

51. The Developer’s tests were performed on each distinct physical hardware platform and also on the VPX-3000 virtualised platform.

52. The Evaluators devised and ran a total of 19 independent functional tests, different from those performed by the Developer. These tests included penetration tests to address potential vulnerabilities considered during the evaluation. No anomalies, exploitable vulnerabilities or errors were detected.

53. The Evaluators’ tests were performed on appliance models MPX 15500-FIPS and MPX 17500, and on virtualised platform VPX-1000, as discussed in Chapter III (in ‘Test Configuration’) of this report.

54. The Evaluators finished running their penetration tests on 2 February 2012.

Vulnerability Analysis

55. 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, in particular the developer's vulnerability analysis.

Platform Issues

56. 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

[AG] Citrix NetScaler Administration Guide – Citrix® NetScaler® 9.3,
Citrix Systems Inc.,
Document code: December 23 2011 04:11:43.

[AFG] Citrix Application Firewall Guide – Citrix® NetScaler® 9.3,
Citrix Systems Inc.,
Document code: January 31 2012 00:15:53.

[ASG] Citrix NetScaler Application Security Guide – Citrix® NetScaler® 9.3,
Citrix Systems Inc.,
Document code: April 28 2011 09:30:50.

[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.

[CCECG] Common Criteria Evaluated Configuration Guide for NetScaler 9.3 Platinum Edition,
Citrix Systems Inc.,
Document code: Feb 9, 2012 11:46:36.

[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.

[CRG] Citrix NetScaler Command Reference Guide – Citrix® NetScaler® 9.3,
Citrix Systems Inc.,
Document code: March 21 2011 06:30:14.

[CR] Common Criteria Certification Report No. CRP262,
UK IT Security Evaluation and Certification Scheme,
CRP262, Issue 1.1, August 2011.

[ETR] Citrix NetScaler Platinum Edition Load Balancer Version 9.3 Evaluation Technical Report,
SiVenture CLEF,
CIN7-TR-0001, Version 1-1, 6 March 2012.

[MG] Citrix NetScaler Migration Guide – Citrix® NetScaler® 9.3,
Citrix Systems Inc.,
Document code: December 5 2011 08:43:00.

[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® 9.3,
Citrix Systems Inc.,
Document code: November 30 2011 01:11:22.

[PCRG] Citrix NetScaler Policy Configuration and Reference Guide – Citrix® NetScaler® 9.3,
Citrix Systems Inc.,
Document code: October 17 2011 02:44:14.

[ST] Common Criteria Security Target for NetScaler Platinum Edition Load Balancer Version 9.3,
Citrix Systems Inc.,
CIN7-ST-0001, Version 1-0, 16 February 2012.

[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-GS] Citrix NetScaler VPX Getting Started Guide – Citrix® NetScaler® VPX^{TM} 9.3,
Citrix Systems Inc.,
Document code: January 11 2012 01:29:10.

VII. ABBREVIATIONS

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

ADNP	Application Delivery Networking Platform
API	Application Program Interface
AppFW	Application Firewall
CLI	Command Line Interface
CRL	Certificate Revocation List
FIPS	Federal Information Processing Standard
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5 (a one-way hash function)
MPX	NetScaler physical hardware platform
NS	NetScaler (platform)
OSI	Open Systems Interconnection
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
VPN	Virtual Private Network
VPX	NetScaler virtual platform
XML	Extensible Markup Language

This page is intentionally blank.