122-B

CERTIFICATION REPORT No. CRP253

Citrix NetScaler Platinum Edition Load Balancer

Version 9.1 (Build 100.3.cl)

running on NetScaler 9010 FIPS, MPX 7000 platform,
MPX 9000 platform, MPX 10000 platform and MPX 12000 platform

Issue 1.0

April 2010

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:	NetScaler Platinum Edition Load Balancer Version 9.1 (Build 100.3.cl)
Platform:	NetScaler 9010 FIPS, MPX 7000 platform, MPX 9000 platform, MPX 10000 platform and MPX 12000 platform
Description:	The NetScaler Platinum Edition Load Balancer Version 9.1 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:	CRP253
Date Certified:	16 April 2010

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 SOG-IS MRA logo which appears below:

- confirms that the certificate has been issued under the authority of a party to an international Mutual Recognition Agreement (MRA) [MRA] designed to ensure that security evaluations are performed to high and consistent standards;
- indicates that it is the claim of the evaluating party that its evaluation and certification processes meet all the conditions of the MRA.

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. Use of the logo of this Agreement does not imply acceptance by other Members of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

CCRA logo **CC logo** **SOG-IS MRA logo**

[1] All judgements contained in this Certification Report, excluding ALC_FLR.2, 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 NetScaler Platinum Edition Load Balancer Version 9.1 (Build 100.3.cl) 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 25 March 2010:

   - **NetScaler Platinum Edition Load Balancer Version 9.1 (Build 100.3.cl)[2] running on NetScaler 9010 FIPS, MPX 7000 platform, MPX 9000 platform, MPX 10000 platform and MPX 12000 platform**

4. Note that there is a single appliance model in each platform listed above. Specifically, the evaluation on the MPX 7000 platform, MPX 9000 platform, MPX 10000 platform and MPX 12000 platform was performed on the appliance models MPX 7500, MPX 9500, MPX 10500 and MPX 12500 respectively.

5. The Developer was Citrix Systems Inc.

6. The NetScaler appliance incorporates three software components that work together to provide secure access to web-based applications from an external network. The three software components are the Load Balancer, Access Gateway, and the Web Application Firewall.

7. TOE Administrators can access the TOE through a direct serial connection. The direct serial connection gives the administrator access to the Command Line Interface (CLI). TOE administrators can also access the TOE from any workstation on the management network using the NetScaler Configuration Utility. The NetScaler Configuration Utility is accessed via a web browser.

8. 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.

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

[2] Hereinafter referred to as Version 9.1.

10. It should be noted that the use of Layer3 routing is excluded from the scope of the evaluation. Details of evaluated configuration requirements are provided in [GDS].

11. 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 2 of [ST].

Security Claims

12. 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 Functions 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.

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

Evaluation Conduct

14. The TOE's SFRs and the security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from that of the previous product version, which had previously been certified [CR] by the UK IT Security Evaluation and Certification Scheme to the CC EAL2 (augmented with ALC_FLR.2) assurance level. It should be noted that additional SFRs relating to the Application Firewall information flow policy were considered in the latest evaluation. For the evaluation of NetScaler Platinum Edition Load Balancer Version 9.1, the Evaluators made some reuse of the previous evaluation results where appropriate, taking the migration from CCv2.3 to CCv3.1 into consideration.

15. 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 March 2010, were reported in the Evaluation Technical Report [ETR].

Conclusions and Recommendations

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

17. Prospective consumers of NetScaler Platinum Edition Load Balancer Version 9.1 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.

18. 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.

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

- TOE consumers should browse to the http://www.citrix.com/ website to initiate download of [GDS], 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 masquerading as the Citrix site.

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

Disclaimers

20. This report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration' of this report.

21. 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.

22. 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.

23. 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.

24. 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

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

Delivery

26. 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.

27. The appliances are shipped to the TOE consumers directly from Citrix Systems Inc. using reputable carriers. Citrix notifies the consumer of the tracking number, which can be used to track the shipment during delivery. 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. Upon receipt the consumer can verify this matches the details of the order placed and also that the listed serial number matches the serial number of the enclosed product. The consumer should also examine the appliance to verify that the tamper seals are not damaged.

28. The consumer should follow the guidance provided in [GDS] to download the certified version of software via the Citrix support website (http://support.citrix.com/). The customer 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 https://support.citrix.com/ website, as detailed in [GDS].

Installation and Guidance Documentation

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

- Guidance Document Supplement, [GDS];
- Citrix NetScaler Hardware Installation and Setup Guide, Citrix NetScaler 9.1, [HIG].

30. The Administration Guide documentation is as follows:

- Citrix Application Firewall Guide, [AFG];
- Citrix NetScaler Administration Guide, [AG];
- Citrix NetScaler Application Security Guide Citrix NetScaler 9.1, [ASG];
- Citrix NetScaler Command Reference Guide, [CRG];
- Citrix NetScaler Traffic Management Guide, [TMG].

III. EVALUATED CONFIGURATION

TOE Identification

31. The TOE is NetScaler Platinum Edition Load Balancer Version 9.1, which consists of the software 'NS9.1: Build 100.3.cl' (downloaded in the file 'build-9.1-100.3_cl.tgz') running on one of the following:

- Appliance Model NetScaler 9010-FIPS;
- MPX 7000 Platform: Appliance Model MPX 7500;
- MPX 9000 Platform: Appliance Model MPX 9500;
- MPX 10000 Platform: Appliance Model MPX 10500;
- MPX 12000 Platform: Appliance Model MPX 12500.

TOE Documentation

32. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in 'Installation and Guidance Documentation') of this report. The relevant guidance documentation (with the exception of [GDS]) is downloaded in the same manner as the firmware image, linked on the same webpage. [GDS] 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

33. 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 1.6.3 and is summarised as follows:

- Content Switching;
- Content Rewrite;
- Caching;
- Compression;
- Web Logging;
- Layer 3 Routing;
- Load Balancing between NetScaler appliances.

34. As detailed in Chapter I (in 'Evaluated Product and TOE Scope') of this document, the 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.

TOE Configuration

35. The evaluated configuration of the TOE is defined in [ST] Section 1.3 and in [GDS]. The following diagram shows the evaluated configuration.

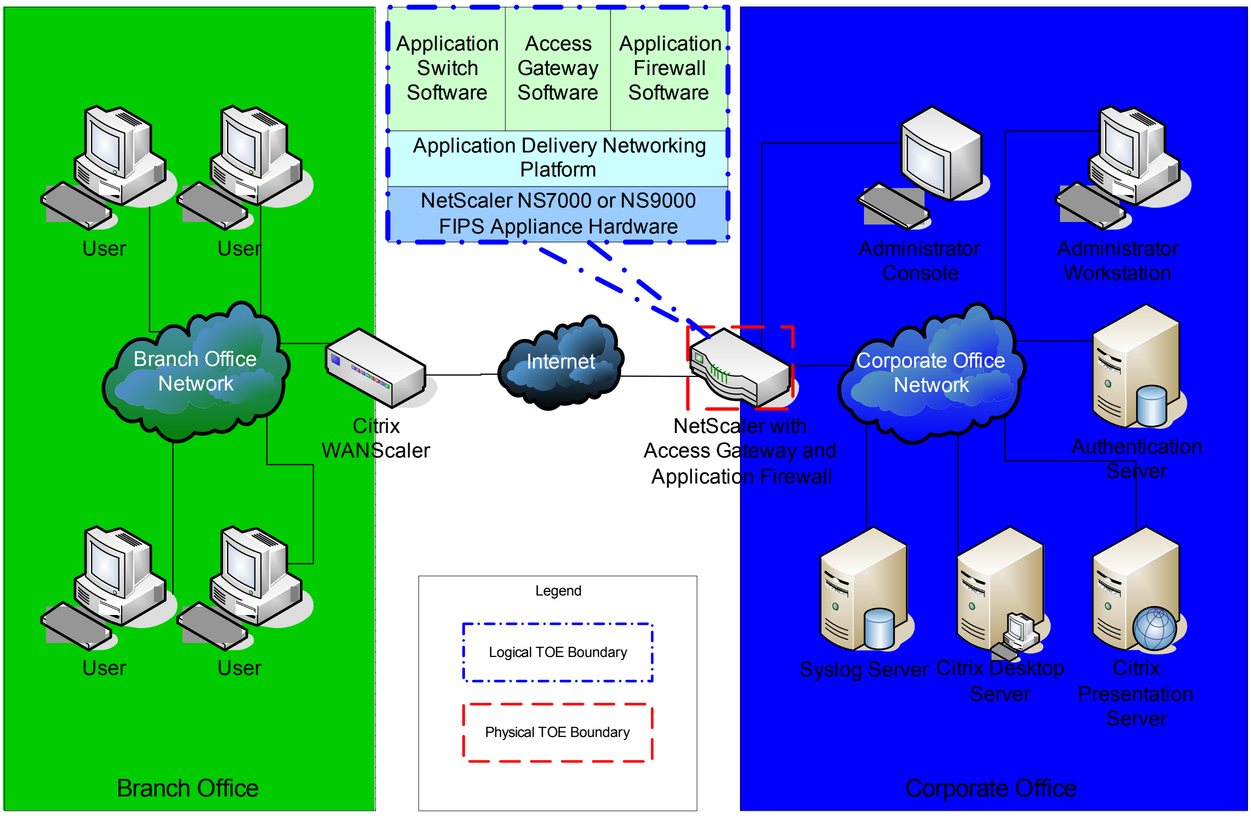

Figure 1 TOE Configuration

Environmental Requirements

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

37. The TOE was evaluated running on the NetScaler 9010 FIPS, MPX 7500, MPX 9500, MPX 10500 and MPX 12500 appliance models.

38. The environmental IT configuration is detailed in [ST] Section 1.5.

Test Configuration

39. The Evaluators performed an analysis of the platform variations between the appliance models being evaluated and determined that it was sufficient to perform the testing on a single platform. Consequently, appliance model MPX 7500 was selected. The test configuration used by the evaluators was consistent with that depicted in 'TOE Configuration' above.

40. The Developers used configurations consistent with that depicted in 'TOE Configuration' above for their testing, and performed their testing on each of the appliances listed in 'Environmental Requirements' above.

IV. PRODUCT ARCHITECTURE

Introduction

41. This Chapter gives an overview of the main TOE 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:

- 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.

- 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.

- The Web Application Firewall component provides firewall protection against attacks at the Application Layer of the Open Systems Interconnection Basic Reference Model. It implements a positive security model, which allows only traffic which adheres to industry standards and best coding practices. All other traffic is treated as malicious and blocked.

43. The above three components run on top of the Application Delivery Networking Platform (ADNP) on the appliances. The ADNP is the specialized kernel and packet-processing engine, which coordinates the operations of the other software components and 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 provide 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 provide access to other file services, such as print services;

- AppFW Learning Subsystem - provides dynamic data firewalling functionality to protect internal networks from attack;

- 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;

- Read-Write Subsystem - stores data in and retrieves data from the Flash Memory Subsystem and handles the configuration file (ns.conf) and SSL certificate keys;

- 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;

- 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. The following diagram shows the high-level design subsystems and their internal and external interfaces.

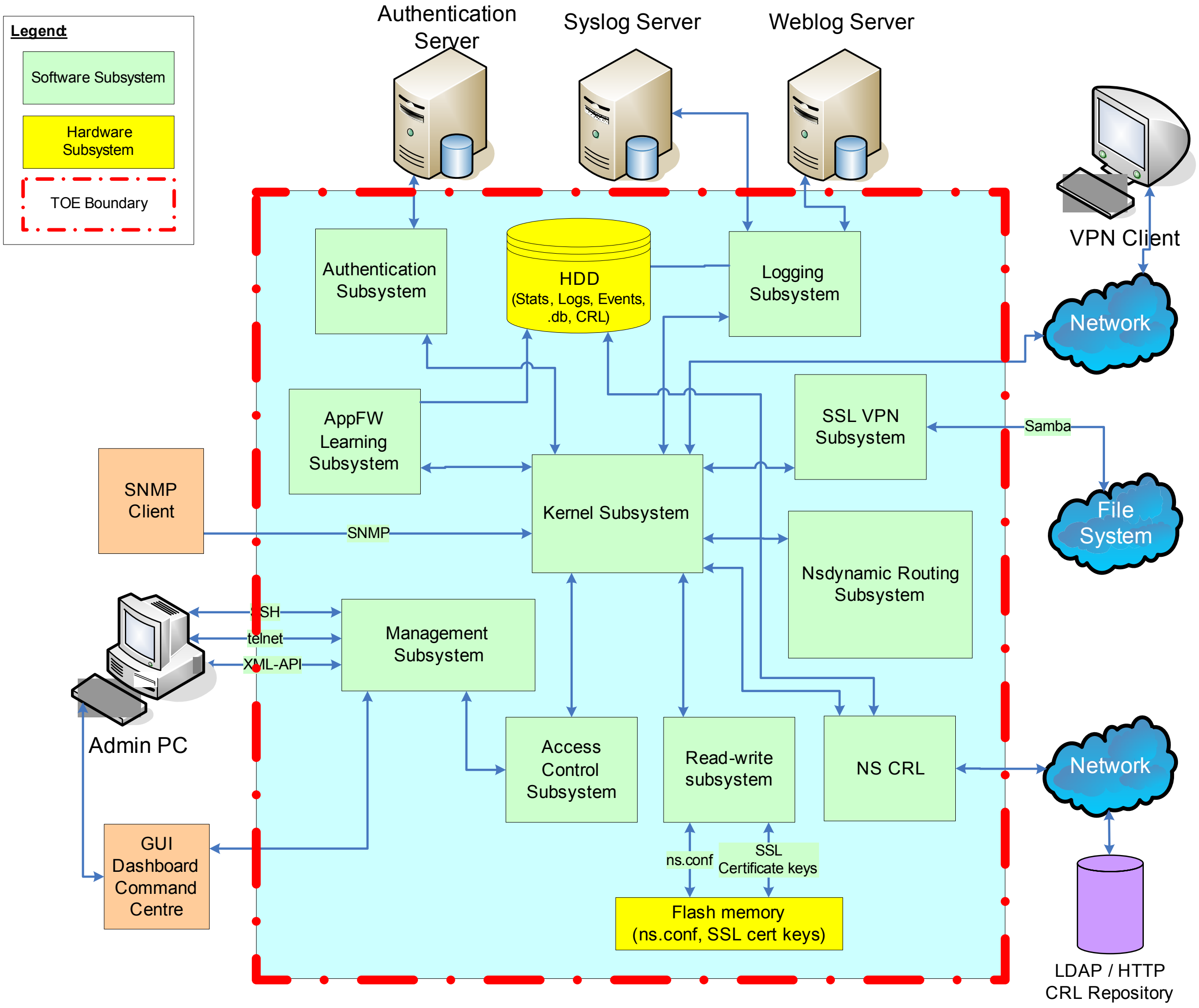

Figure 2 TOE Subsystem and external interfaces

TOE Dependencies

46. The TOE dependencies on the IT environment are identified in Chapter III 'Environmental Requirements'.

TOE Interfaces

47. The external TOE Security Functions Interface (TSFI), as shown in Figure 2 above, are:

- 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;

- Apache Interface – used for management (using XML-API);

- Command Line Interface (SSH, Telnet) – used for management;

- GUI Dashboard Command Centre Interface – used for management;

- SNMP Interface – used to provide status information to monitoring IP devices on the network.

V. TOE TESTING

TOE Testing

48. 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.

49. The Developer's tests were performed on all of the appliances included in the evaluation as detailed in Chapter III (in 'Test Configuration') of this report.

50. The Evaluators devised and ran a total of 17 independent 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. The Evaluator's tests were performed on appliance model MPX 7500 as discussed in Chapter III (in 'Test Configuration') of this report.

51. The Evaluators finished running their penetration tests on 15th March 2010.

Vulnerability Analysis

52. 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

53. The NetScaler 9010-FIPS, MPX 7500, MPX 9500, MPX 10500 and MPX 12500 appliance models are within the scope of the TOE. No platform issues were identified.

VI. REFERENCES

[AFG] Citrix Application Firewall Guide,
Citrix Systems Inc.,
Version 9.1, June 2009.

[AG] Citrix NetScaler Administration Guide,
Citrix Systems Inc.,
Version 9.1, June 2009.

[ASG] Citrix NetScaler Application Security Guide, Citrix NetScaler 9.1,
Citrix Systems Inc.,
June 2009.

[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. CRP247,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, August 2008.

[CRG] Citrix NetScaler Command Reference Guide,
Citrix Systems Inc.,
Version 9.1, June 2009.

[ETR] Evaluation Technical Report,
SiVenture CLEF,
LFV/T008/ETR, Issue 1.1, 31 March 2010.

[GDS] NetScaler Platinum Edition Load Balancer Version 9.1, Guidance Document Supplement,
Corsec Security Inc. (on behalf of Citrix Systems Inc.),
Version 1.0, March 2010.

[HIG] Citrix NetScaler Hardware Installation and Setup Guide, Citrix NetScaler 9.1,
Citrix Systems Inc.,
Version 9.1, July 2009.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee of Agreement Group,
Senior Officials Group – Information Systems Security,
Version 2.0, April 1999.

[ST] NetScaler Platinum Edition Load Balancer Version 9.1 Security Target,
Citrix Systems Inc.,
Issue 1.0, 23 March 2010.

[TMG] Citrix NetScaler Traffic Management Guide,
Citrix Systems Inc.,
Version 9.1, June 2009.

[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 4.2, December 2009.

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

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML, LAN, PC); standard CC 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
CRL	Certificate Revocation List
HDD	Hard Disk Drive
FIPS	Federal Information Processing Standards
LDAP	Lightweight Directory Access Protocol
MD5	Message-Digest algorithm 5
NS	NetScaler (platform)
SSL	Secure Sockets Layer
VPN	Virtual Private Network