122-B

CERTIFICATION REPORT No. CRP247

Citrix NetScaler
Version 8.0 (Build 54.6)
running on NS7000 and NS9010-FIPS

Issue 1.0

August 2008

UK Certification Body
CESG, Hubble Road
Cheltenham, GL51 0EX
United Kingdom

**ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement 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 carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

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 Version 8.0 (Build 54.6)
Platform	NS7000 and NS9010-FIPS
Description	The TOE is a dedicated application performance accelerator incorporating a Secure Sockets Layer (SSL) Virtual Private Network (VPN) with policy-based access control and an application-level firewall.
CC Part 2	Conformant
CC Part 3	Conformant
EAL	EAL2 augmented by ALC_FLR.1
SoF	SoF-Basic
PP Conformance	None
CLEF	SiVenture
Date Certified	28 August 2008

The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 [UKSP01] and 02 [UKSP02P1, UKSP02P2]. The Scheme has established a 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[1] 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 carried out properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

Trademarks:

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

[1] All judgements contained in this Certification Report are covered by the Recognition Arrangement.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of NetScaler Version 8.0 to the Sponsor, Citrix Systems Inc., as summarised in the Certification Statement, 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; and the Common Criteria Guidance Supplement [CCGS].

Evaluated Product and TOE Scope

3. The following product completed evaluation to CC **EAL2** augmented by ALC_FLR.1 on 28 August 2008:

   - **NetScaler Version 8.0 (Build 54.6)**

4. The Developer was Citrix Systems Inc.

5. The NetScaler appliance incorporates three software components that work together to provide secure access to web-based applications, such as the Citrix Desktop Server or Presentation Server, from an external network. The three software components are the Application Switch, the Access Gateway and the Application Firewall. These run on top of the Application Delivery Networking Platform (ADNP) on the NetScaler NS7000 or NS9010-FIPS Appliance Hardware. (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.)

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 ‘Evaluated Configuration’.

7. The security functions specified for evaluation focus on the security of the TOE administrative interfaces. The TOE provides many features that focus on protecting user data, but the security of these features (as described in Section 2.2 of [ST]) is beyond the scope of this evaluation as specified in Section 3.2 of [ST].

8. The connection between the TOE and an (optional) external authentication server is assumed to be protected from tampering, as detailed in [CCGS].

9. An overview of the TOE and its security architecture can be found in Chapter IV ‘Product Architecture’. Configuration requirements are specified in Section 2.1 and 2.3 of [ST].

Protection Profile Conformance

10. The Security Target [ST] is does not claim conformance to any protection profile.

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) that refine 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 TOE security policies are detailed in the ST [ST].

13. The environmental assumptions related to the operating environment are detailed in Chapter III under 'Environmental Requirements'.

Strength of Function Claims

14. The minimum Strength of Function (SoF) was claimed to be SoF-Basic. This is claimed for the Identification and Authentication function (relating to FIA_UID.2 and FIA_UAU.2). The Evaluators have determined that this claim was met.

Evaluation Conduct

15. The Certification Body monitored the evaluation which was carried out 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 August 2008, were reported in the Evaluation Technical Report [ETR].

Conclusions and Recommendations

16. The conclusions of the Certification Body are summarised in the Certification Statement on page 2.

17. Prospective consumers of NetScaler Version 8.0 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST] and CC Configuration Guide Supplement [CCGS]. 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' below includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

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

- **TOE administrators should take note of the recommendations and guidance provided in [CCGS] in conjunction with application notes in the ST, in particular the guidance provided in Sections 5.1 and 7 of [CCGS].**

- **The consumer of this TOE should note that it is the consumer's responsibility to ensure adequate assurance is obtained in the implementation of cryptographic algorithms used in the instantiation of the TOE.**

Disclaimers

20. This Certification Report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration'.

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 Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) 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. 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 by a Scheme-approved Assurance Continuity process.

II. TOE SECURITY GUIDANCE

Introduction

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

Delivery

23. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

24. The TOE hardware is shipped to the consumer using UPS or FedEx carriers. Consumers should verify the authenticity of the received product by performing the following checks:

- Verify the shipping label on the outside of the package lists the exact product ordered, and the listed serial number matches the serial number of the enclosed product.
- Verify that the tamper seals are not damaged**.**
- Verify the tracking number on the package is the same as the shipping number provided by Citrix (via email).

25. The TOE hardware ordered comes pre-installed with the latest version of the product software, which may or may not be the evaluated version of the TOE. Consumers should download the software portion of the TOE from http://support.citrix.com, as detailed in [READ]. This support website is protected by login credentials to restrict access to legitimate users only, and an SSL encrypted session to ensure integrity is maintained during download. The customer is able to further verify the integrity of the downloaded image by performing an MD5 hash of the software image and comparing it to the values posted in the checksum file associated with the relevant firmware version, i.e. “checksum_8_0_54_6_md5.txt”.

Installation and Guidance Documentation

26. The Installation and Configuration documentation is as follows:

- Administrator’s Guide [AG], specifically Section 3.
- Common Criteria Guidance Supplement [CCGS].
- NetScaler Installation and Migration Notes (ReadMeFirst) [READ].

27. The Administration Guide documentation is as follows:

- Common Criteria Guidance Supplement [CCGS] (this takes precedence over the other Administration Guide documentation).

- Command Reference Guide [CRG].
- Administrator’s Guide [AG].

28. The User Guide documentation is provided by the TOE screen prompts displayed to the user.

III. EVALUATED CONFIGURATION

TOE Identification

29. The TOE is NetScaler Version 8.0, which consists of

- Citrix NetScaler Application Switch with Access Gateway Enterprise Edition and Application Firewall software version 8.0 (Build 56.4).
- NetScaler appliances NS7000 and NS9010-FIPS.

TOE Documentation

30. The relevant guidance documentation for the evaluated configuration is identified above under ‘Installation and Guidance Documentation’.

TOE Scope

31. The TOE Scope is defined in [ST] Section 2.3. Functionality that is outside the scope of the TOE is described in [ST] Sections 2.2 and 3.2.

32. The Security Functional Requirements (SFRs) focus on the security of the TOE administrative interfaces. The TOE provides many features that focus on protecting user data, but the security of these features is beyond the TOE scope.

TOE Configuration

33. The evaluated configuration of the TOE is defined in [ST] Section 2.1 and in [CCGS]. The following diagram shows the evaluated configuration.

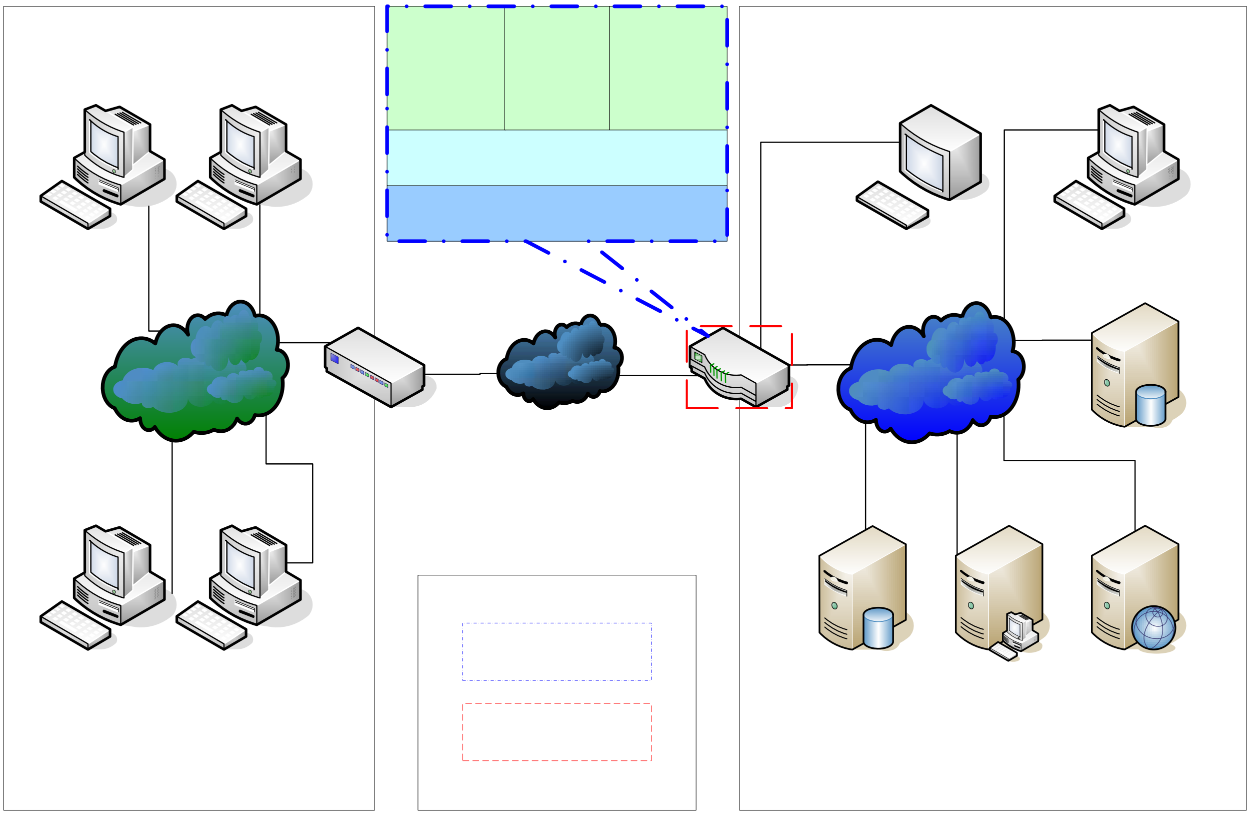

Figure 1 TOE evaluated configuration

Environmental Requirements

34. The environmental assumptions for the TOE are stated in [ST] Section 3.1. The SFR for the IT environment is stated in [ST] Section 5.2.

35. The environmental IT configuration is as follows:

- Administrator console and workstation for management;
- Application server(s);
- VPN client(s);
- Network(s) (including the Internet and the Corporate Office Network);
- (Optional) Authentication server (RADIUS, LDAP, TACACS+, or NT4).

Test Configuration

36. The evaluators analysed the reliance on the TOE platforms to support the TOE Security Functions (TSFs) and determined that only the kernel (considered to be a hardware, firmware and software subsystem of the TOE) was relied upon. The implementation of the

kernel is common between the platforms. Therefore, it was sufficient to perform the testing on a single platform.

37. The following configuration was used by the Developers for testing

- 1xNS9010-FIPS running NetScaler 8.0 Build 54.6.

38. The following configuration was used by both the Developers and the Evaluators for testing

- 1xNS7000 running NetScaler 8.0 Build 54.6.

IV. PRODUCT ARCHITECTURE

Introduction

39. This Chapter gives an overview of the main architectural features. Details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

Product Description and Architecture

40. The architecture incorporates three software components that work together to provide secure access to web-based applications. The three software components are:

- Application Switch, which manages the connections between clients and servers. Clients establish a connection with the NetScaler rather than directly to a server. When the NetScaler receives application requests from the client, it establishes a connection with the appropriate application server. This allows the Application Switch to sort and prioritize application requests from multiple clients and requires only a single connection on the application server to handle requests from multiple clients. Additionally, it utilizes Transmission Control Protocol (TCP) optimizations and several acceleration technologies to accelerate application performance.

- Access Gateway, which is an SSL VPN providing 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. It can also be configured to have the VPN client run a check on the user's computer to ensure that the latest anti-virus updates are installed before allowing access to mission critical systems.

- Application Firewall, which provides firewall protection against attacks at the Application Layer of the Open Systems Interconnection Basic Reference Model (OSI 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. This model does not require the use of signatures and can protect against zero-day attacks.

41. These run on top of the Application Delivery Networking Platform (ADNP) on the NetScaler NS7000 or NS9010-FIPS Appliance Hardware. (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

42. 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 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 (CRLs);
- 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.

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

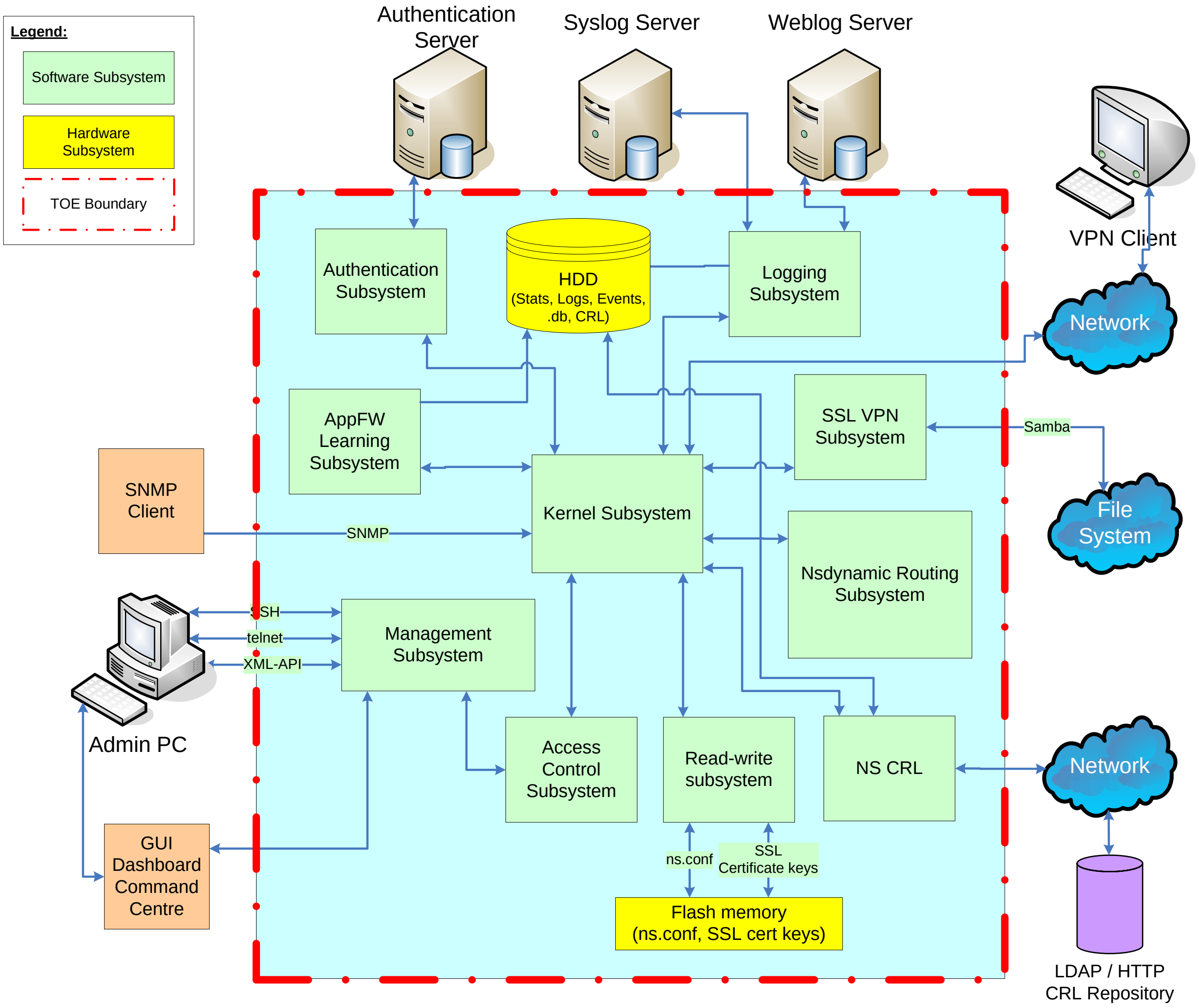

Figure 2 TOE High-Level Design subsystems and interfaces

TOE Dependencies

44. The TOE dependencies are specified in Chapter III ‘Evaluated Configuration’ and are described in [CCGS].

TOE Interfaces

45. The external TSFI is described as follows and shown in Figure 2 above:

- 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 syslog and weblog servers (use of which is excluded from evaluated configuration);

- 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

46. The Developer’s tests covered all SFRs, all TOE high-level subsystems (as identified under ‘TOE Design Subsystems’ in Chapter IV), all SFs and the TSFI (as identified under ‘TOE Interfaces’ in Chapter IV). The tests were performed on both the NetScaler NS7000 and NS9010-FIPS appliances. The test configurations were the same as the evaluated configuration, as described in ‘TOE Configuration’ in Chapter III.

47. The Evaluators devised and ran 15 independent functional tests, different from those performed by the Developer. These tests included penetration tests devised by the evaluators to address potential vulnerabilities considered during the evaluation. As a result of this testing the evaluators identified the need for additional guidance in [CCGS], to be used in conjunction with the application notes in the ST, concerning the presence of sensitive information in audit logs which therefore requires the prevention of unauthorized access to a log file. (The importance of [CCGS] is noted as part of the Evaluator recommendations in paragraph 19 above). The Evaluator’s tests were performed on the NetScaler NS7000 appliance using the evaluated configuration described in ‘TOE Configuration’ in Chapter III.

48. In addition the Evaluators identified the following open bug reports which affect the behaviour of the TOE, while not undermining the implementation of any SFRs:

- Bug 36282: Although a username of 127 characters in length can be created for an aaa user, the user will be unable to login as the GUI will only accept 30 characters of the username.

- Bug 39944: A non-root user who does not have permission to execute “sh version” has to use the CLI, rather than the GUI, to view the historical audit messages.

Vulnerability Analysis

49. The Evaluators’ vulnerability analysis, which preceded penetration testing, was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables.

Platform Issues

50. The NetScaler NS7000 and NS9010-FIPS appliances are within the scope of the TOE. No platform issues were identified. The Evaluators observed during testing that the NetScaler NS7000 and NS9010-FIPS appliance provided the same security functionality.

VI. REFERENCES

[A&R] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
Issue 1.4, January 2008.

[AG] Citrix Access Gateway Enterprise Edition Administrator’s Guide,
Citrix Systems Inc.,
Document code March 12, 2007 (MS).

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2005-08-001, Version 2.3, August 2005.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-002, Version 2.3, August 2005.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-003, Version 2.3, August 2005.

[CCGS] NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 Common Criteria Guidance Supplement,
Citrix Systems Inc.,
Version 1.0, 25 August 2008.

[CEM] Common Methodology for Information Technology Security Evaluation,
Common Criteria Maintenance Board,
CCMB-2005-08-004, Version 2.3, August 2005.

[CRG] Citrix NetScaler Application Switch Command Reference Guide Release 8.0,
Citrix Systems Inc.,
Part No. NS_CRG_80_0507, May 2007.

[ETR] NetScaler Application Switch with Access Gateway Enterprise Edition and Application Firewall Version 8.0 Evaluation Technical Report,
SiVenture,
CINN-TR-0001, Version 1.0, 28 August 2008.

[READ] Citrix NetScaler Application Switch NS Installation and Migration Notes (ReadMeFirst) Release 8.0,
Citrix Systems Inc.,
NS-MIG-80-0507, May 2007.

[ST] Security Target,
NetScaler Application Switch with Access Gateway Enterprise Edition and Application Firewall Version 8.0,
Citrix Systems Inc.,
Version 1.1, 16 July 2008.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.1, March 2006.

VII. ABBREVIATIONS

This list does not include well known IT terms (such as GUI, HTML, LAN, PC) or standard Common Criteria abbreviations (such as TOE, TSF; see Common Criteria Part 1 [CC1]) or Scheme abbreviations (such as CESG, CLEF; see [A&R]).

ADNP	Application Delivery Networking Platform
BGP	Border Gateway Protocol
CRL	Certificate Revocation List
FIPS	Federal Information Processing Standards
LDAP	Lightweight Directory Access Protocol
MD5	Message-Digest algorithm 5
NS	NetScaler (platform)
OSPF	Open Shortest Path First
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
SSL	Secure Sockets Layer
TACACS+	Terminal Access Controller Access-Control System Plus
VPN	Virtual Private Network

This page is intentionally blank.