KECS-CR-06-13

Nexg Co., LTD. VForce 2200 V1.0

Certification Report

Certificate Number: KECS-NISS-0053-2006

October 2006

National Intelligence Service

IT Security Certification Center

This document is the certification report on VForce 2200 V1.0 of Nexg Co., LTD.

Certification Body

National Intelligence Service IT Security Certification Center

Evaluation Body

Korea Information Security Agency

Table of Contents

1. Executive Summary

This report documents the certification result of the EAL3+ evaluation of VForce 2200 V1.0 with regard to the Common Criteria for Information Technology Security Evaluation (Announcement No. 2005-25 by Ministry of Information and Communication; CC hereinafter). It presents the evaluation results, their validation, and the conformance results.

The Korea Information Security Agency (KISA) has finished the evaluation of the VForce 2200 V1.0 on the 22th of Sept. 2006. This report is written based on the Evaluation Technical Report produced and provided by the KISA.

The evaluation concludes that the TOE satisfies the CC part 2 and the EAL3 of the part 3 assurance requirements with augmenting ADV_IMP.2, ADV_LLD.1, ALC_TAT.1, ATE_DPT.2, AVA_VLA.2; thus, it is assigned the verdict 'pass' on the basis of the paragraph 191 of the CC part 1. In addition, the TOE satisfies the Firewall Protection Profile V1.1 (April. 24, 2003) and the VPN Protection Profile V1.1 (April. 24, 2003).

VForce 2200 V1.0 (the TOE), developed by Nexg Co., LTD, is an appliance equipment that provides the firewall and VPN functions. The TOE is installed on the single connection point that separates the external and internal network, and is installed and administered through the CLI (Command Line Interface) or GUI(Graphic User Interface). All of security functions of the TOE are included in the evaluation scope, and the main security functions are as follows:

- Security Management
- Discretionary · Mandatory Access Control
- User authentication using proxy(HTTP, Telnet, FTP)
- Confidentiality and Integrity for the transmitted data
- Network Address Translation (NAT)
- User/Administrator identification and authentication
- Generation and protection of the security audit data
- Integrity of execution and configuration files

The certification body has examined the evaluation activities and testing procedures of the evaluator; provided the guidance regarding the technical problems and evaluation procedures; reviewed each evaluation work package and the

evaluation technical report. The certification body has confirmed that the evaluation results assure that the TOE meets all of the security function requirements and assurance requirements described in the ST. As a result, the certification body has certified that the observations and evaluation results by the evaluator are accurate and reasonable; and that each verdict on each work package of the evaluator is correct.

Certification Validity: The information in this report guarantees that VForce 2200 V1.0 obtained neither approval for use nor quality assurance from the Government Agency of the Republic of Korea.

2. TOE Identification

[Table 1] describes the information about the TOE identification.

[Table 1] TOE Identification

Evaluation Guidance	Korea IT Security Evaluation and Certification Guidance (2005. 5. 21) Korea IT Security Evaluation and Certification Scheme (2005. 12. 26)
TOE	VForce 2200 V1.0
Protection Profile	Firewall Protection Profile V1.1(2003. 4. 30) VPN Protection Profile V1.1(2003. 4. 30)
Security Target	VForce 2200 V1.0 ST V1.1(2006. 7. 20), Nexg Co., LTD
ETR	VForce 2200 V1.0 ETR, V1.1(2006. 9. 20)
Conformance Result of the Evaluation	Conformance to the CC V2.3 part 2 Conformance to the augmented part 3 (ADV_IMP.2, ADV_LLD.1, ALC_TAT.1, ATE_DPT.2, AVA_VLA.2)
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation V2.3 (2005. 8)
Evaluation Methodology	Common Methodology for Informations Technology Security Evaluation V2.3 (2005. 8)
Sponsor	Nexg Co., LTD
Developer	Nexg Co., LTD
Evaluators	KISA IT Security Evaluation Center, Evaluation Team I Byung Kwon Lee, Hyun Jung Lee, Jun Woo Park
Certification Body	National Intelligence Service

[Table 2] describes the system specification of the TOE.

[Table 2] VForce 2200 V1.0 System Specification

Item		Specification
CPU		- Intel IV 2.26 GHz
RAM		- 256MB
IDE Flash Disk		- 16MB (Firmware, Configuration DB)
Interface	Network	- 10/100 Base TX : 6 port
	Management	- Serial : 1 - AUX : 1
O/S		- VOS v3.0(dedicated O/S)

3. Security Policy

The TOE operation conforms to the security policies as follows:

Audit	To trace responsibilities of all security-related behaviors, all security-related events shall be stored, maintained, and reviewed.
Trusted Management	The authorized administrator shall manage the TOE in a secure manner.
Confidentiality	If the network traffic transmitted to/from the counterpart of the TOE is specified on the TOE security policy, the traffic shall be encrypted or decrypted by the TOE.
Cryptographic	The cryptographic algorithm and module used in the TOE must be approved by the Director of National Intelligence Service.
Plain Text Transmission	All network traffic other than those transmitted to/from the counterpart of the TOE are allowed to be transmitted without encryption/decryption according to the TOE security policy.

4. TOE Assumptions and Scope

4.1 Assumptions

The TOE installation and operation shall be conformance to the assumptions as follows:

A.Physical Security	The TOE is installed in a physically safe environment accessible only by authorized administrators.
A.Security Maintenance	Upon changes in the network such as configuration changes, increase or decrease of hosts, and service increase/decrease, the new environment and the new security policy shall be immediately reflected in the TOE operation policy to provide a consistent level of security.
A.Trusted Administrator	The authorized administrator of the TOE shall not have any malicious intention, receive proper training on TOE management, and follow the administrator guidelines.
A.Operating System Reinforcement	(For a VPN gateway) Unnecessary services or means shall be removed from the operating system, and security shall be enhanced to better protect against vulnerabilities in the operating system thereby ensuring its reliability and stability. (In case of a VPN client, the sub operating system of the TOE is secure and reliable.)
A.Single Point Of Connection	All external networks and internal networks communicate with each other only through the TOE.
A.Security Policy	The TOE and its counterpart must use interchangeable security policies that share the same security policy and minor differences.
A.Trusted Server	Trusted servers are installed outside the TOE for maximum TOE performance. Such servers include the Network Time Protocol (NTP) server for reliable time management and the remote security management system.
A.Trusted Channel	The communication data between the TOE and the administrator is transmitted through a secure channel established by OpenSSL and the certificate for the OpenSSL is managed in a secure manner.
A.Trusted Storage	Audit records related to the TOE are stored, and the storage is maintained and operated in a secure manner.

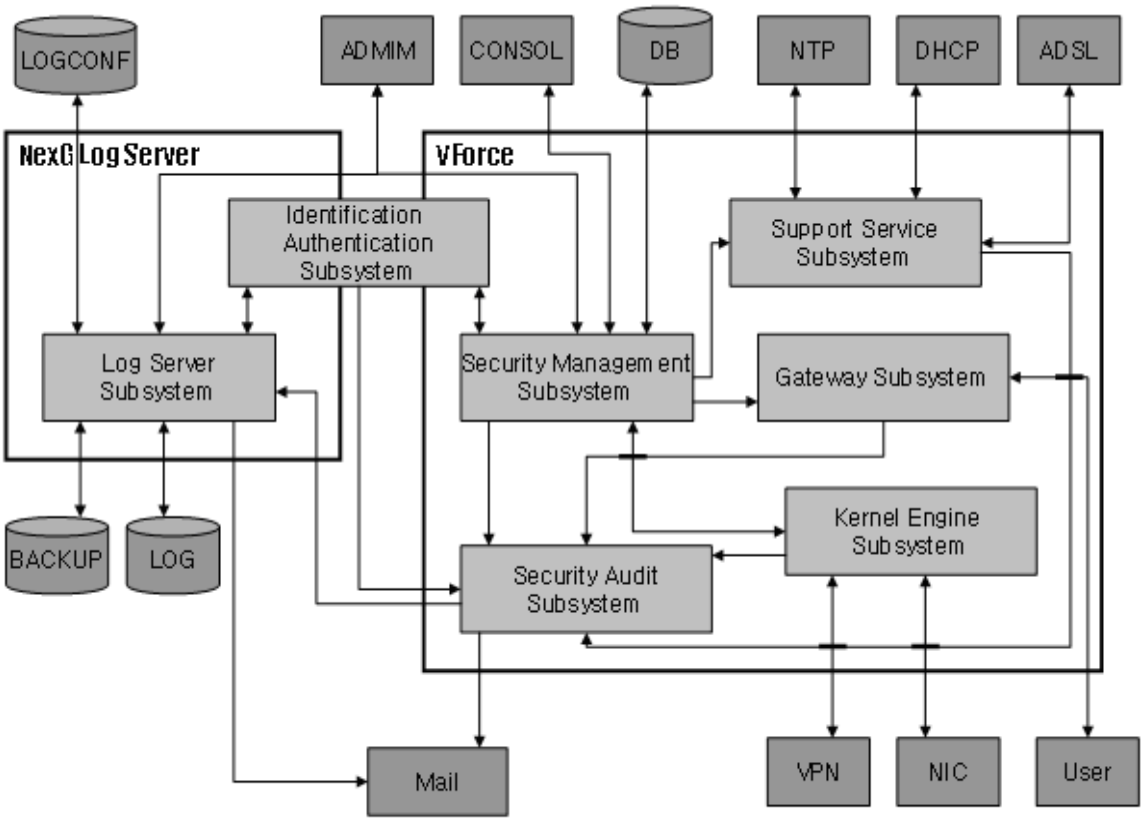
4.2 Threats

The TOE provides countermeasures not only for security threats such as trying to violate the asset of TOE but also a direct physical attack that makes the security functions ineffective or bypasses. It also provides measures of logical/physical attacks made by threat agents with medium-level expertise, resources, and motivation.

All security objectives and security policies are described to provide a means to counter an identified security threat.

5. TOE Information

The TOE provides security functions such as running secure application with the following subsystems.



[Figure 2] Subsystems of the TOE

The TOE comprises 7 subsystems providing access control, proxy, confidentiality and integrity of the transmitted data, and the summary of each subsystem is as follows:

- Security Management

The security management subsystem provides Graphic User Interface (GUI) for the administrator to manage security policies applying to the kernel engine and gateway subsystems and create, modify, delete TSF data.

- Security Audit

The security audit subsystem forwards audit record received from each subsystem to the external log server and stores in the buffer temporarily.

The administrator can view audit records in the buffer by type through security management screen.

- Log Server

The log serve subsystem stores audit records generated by the security audit subsystem in the log server, and provides the search and statistics functions for the records.

- Kernel Engine

The kernel engine subsystem allows traffic from the trusted network applying the access control and cryptographic function for the incoming traffic that conform to the security policy set by the administrator. Network Address Translation (NAT) is also provided to protect internal network users from attempts to guess the private IP address.

- Identification and Authentication

The identification and authentication subsystem identifies and authenticates general users and authorized administrators using static password or one-time password.

- Supporting Service

The supporting service subsystem checks the status of network interfaces to support a variety of network environments, and provides the management function for network interfaces, network routing tables, arp tables.

- Gateway

Proxy provides user authentication for HTTP, TELNET and FTP services.

6. Guidance

The TOE provides the following guidances:

- VForce 2200 V1.0 Administrator Guide V1.1, Mar. 31, 2006
- VForce 2200 V1.0 Installation Guide V1.1, Nov. 15, 2005
- VForce 2200 V1.0 User Guide V1.1, Mar. 31 2006

7. TOE Test

7.1 Developer Testing

- **Test Method**

The developer produced the test cases, considering the security function of the TOE. Each test case is described in test documentation. Each test case described in the test documentation includes the following items in detail:

- Test No./Tester : The identifier of the test and the developer who participated in testing
- Test Purpose : Describe the purpose of the test including security function or modules of the test
- Test Configuration : Detailed test configuration to carry out the testing
- Test Procedure : Detailed procedure to test the security function
- Expected Result : The expected test result when carrying out the test procedure
- Actual Result : The test result when carrying out the test procedure
- Comparison: The result of comparison between the expected and the actual result

The evaluator evaluated the validity of the test reviewing the test configuration, test procedure, test scope analysis of the test documentation and testing low-level design. The evaluator also assured that the developer's test and test results are adequate for the evaluation configuration.

- **Test Configuration**

The test configuration described in the test documentation includes the detailed configuration such as the organization of network for the test, the TOE, PCs, servers, and test tools.

- **Test Scope Analysis/Low-level Design Test**

The detailed evaluation results are described in the evaluation result of ATE_COV and ATE_DPT.

- **Test Result**

The test documentation describes the expected and actual result of each test. The actual result can be verified using not only GUI of the TOE but also the audit record.

7.2 Evaluator Testing

The evaluator installed the TOE by using the evaluation configuration and tools identical to the developer testing, and tested all of test cases provided by the developer. The evaluator assured that the actual test result was identical to the expected result.

In addition, the evaluator created additional evaluator test cases on the basis of developer test, and verified that the actual test result was identical to the expected one.

The evaluator carried out the vulnerability test, and verified no vulnerability for malicious use in the evaluation configuration found.

The evaluator's test result assured that the TOE works normally as described in the design documentation.

8. Evaluated Configuration

The network configuration for the evaluation is separated into the external and internal network. The following hardware is used for the evaluation configuration;

- Computer : 9 sets (6 computer sets for internal and external network)
- CPU : 600MHz or higher
- RAM : 256MB or more
- Hard Disk : 10GB or more

The following software are used for the evaluation configuration;

- Hancom Linux 2.2 (Linux Kernel 2.4.13)
- Windows 2000 Server (SP4, the latest updates)
- Solaris 9 (SunOS 5.9)

All security functions provided by the TOE are included in the evaluation scope, and the evaluation configuration is based on the detailed security attributes and configuration of each security function.

9. Evaluation Result

The latest the Common Criteria for Information Technology Security Evaluation and Common Methodology for Informations Technology Security Evaluation are applied to the evaluation It concludes that the TOE satisfies the CC V2.2 part 2 and EAL3 of the CC V2.2 part3 assurance requirements with ADV_IMP.2, ADV_LLD.1, ALC_TAT.1, ATE_DPT.2, AVA_VLA.2 augmented. The detailed information regarding the evaluation result is described in the ETR.

- ST Evaluation (ASE)

The evaluator applied the ASE sub-activities described in the CC to the ST evaluation. The TOE description is coherent and consistent internally and with the other parts of the ST. The statement of TOE security environment provides a clear and consistent definition of the security problem that the TOE and its environment is intended to address. The security objectives are described completely and consistently, and to determine whether the security objectives counter the identified threats, achieve the identified organizational security policies and are consistent with the stated assumptions. The TOE security requirements and the security

requirements for the IT environment are described completely and consistently, and that they provide an adequate basis for development of a TOE that will achieve its security objectives. The TOE summary specification provides a clear and consistent high-level definition of the security functions and assurance measures, and that these satisfy the specified TOE security requirements. The ST is a correct insanitation of PPs for which compliance is being claimed.

- Configuration Management Evaluation (ACM)

The evaluator applied the ACM sub-activities described in the CC to configuration management evaluation of the TOE. The configuration management documentation describes that configuration list, identification rules, modification control rules. Creation and modification of all source files and development documents proceed in the configuration management system.

- Delivery and Operation Evaluation (ADO)

The evaluator applied the ADO sub-activities described in the CC to the delivery and operation evaluation. Delivery and operation documentation describes the procedures and steps for the secure delivery, installation, operation, and ensure to maintain security while the TOE is in transit, installation, start-up operation. A development site visit verified that all development phases are done by delivery and operation documentation.

- Development Evaluation (ADV)

The evaluator applied the ADV sub-activities described in the CC to the development evaluation. Development documentation presents TOE security functional requirements from TSS level in the ST to implementation level using functional specification, high-level design, and low-level design, and implementation representation. The documentation describes requirements correctly and completely by using correlation between development representation in each development phase.

- Guidance Evaluation (AGD)

The evaluator applied the AGD sub-activities described in the CC to the guidance evaluation. The user guidance describes how to use the user interface provided by the TOE representing examples, and administrator guidance describes how to access the security management interface and the information on each menu and notes with examples. The evaluation verified that the user/administrator guidance are complete and correct.

- Life Cycle Support Evaluation (ALC)

The evaluator applied the ALC sub-activities described in the CC to the life cycle support evaluation. The life-cycle support documentation presents security measures such as procedures, policies for overall development phases and tools and techniques are used to protect the development environment. A development site visit verified that the development environment were protected as the life-cycle support documentation.

- Tests Evaluation (ATE)

The evaluator applied the ATE sub-activities described in the CC to the test evaluation. The test documentation describes the purpose, procedure, and result of the test for security functions specified in the ST. The evaluator verified that the security functions operate correctly by repeating function and module tests on each development phase. The evaluator testing verifies the completeness of the developer testing.

- Vulnerability Evaluation (AVA)

The evaluator applied the AVA sub-activities described in the CC to the vulnerability evaluation. The vulnerability documentation describes the analysis of the vulnerability, potential misuse, and measures completely and correctly. the independent vulnerability test by the evaluator verified the correctness of the vulnerability analysis by the developer. The evaluation of strength of TOE security functions describes that the strength of TOE security function meets or exceeds the minimum strength level defined in the PP/ST.

10. Recommendations

- VForce 2200 V1.0 provides not content-based control function like blocking a command but the proxy authentication service for HTTP, TELNET, and FTP services. Therefore, It is necessary to find the vulnerability of the system by checking the configuration of the servers and update status periodically.

- When the audit trail crosses the threshold set by the administrator, the security functions of VForce 2200 V1.0 are suspended, so periodic monitoring of the audit trail is necessary. In addition, the log server must be managed in a secure manner by installing and operating it in the trusted network.

- VForce 2200 V1.0 is able to not prevent but detect some intrusion attempts such as port scanning and fragmenting packets, so the administrator shall analyze the intrusion detection result, and configure access control to protect the internal network against attackers.

11. Acronyms and Glossary

The following acronyms are used in the certification report.

(1) Acronyms

CR	Certification Report
EAL	Evaluation Assurance Level
IT	Information Technology
KECS	Korea IT security Evaluation and Certification Scheme
TOE	Target of Evaluation
HTTP	Hypertext Transfer Protocol
FTP	File Transfer Protocol

(2) Glossary

TOE	An IT product or system and its associated guidance documentation that is the subject of an evaluation
Audit Record	Audit data to save an auditable event relevant to the TOE security
User	Any entity (human or external IT entity) outside the TOE that interacts with the TOE
Authorized Administrator	Authorized user that can manage the TOE in accordance with the TSP
Authorized User	User that can run functions of the TOE in accordance with the TSP
Identity	A representation uniquely identifying an authorized user
Authentication Data	Information used to verify the claimed identity of a user
External IT Entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE
Asset	Information and resources to be protected by the countermeasures of a TOE

Daemon	A process that runs in the background and respond periodical service requests
NTP	An internet standard protocol that assures accurate synchronization to the millisecond of computer clock times in a network of computers

12. References

The certification body has used the following documents to produce the certification report:

[1] Common Criteria for Information Technology Security Evaluation (May. 21, 2005.)
[2] Common Methodology for Information Technology Security Evaluation V2.3
[3] Firewall Protection Profile V1.1 (April. 30, 2003)
[4] VPN Protection Profile V1.1 (April. 30, 2003)
[5] Korea IT Security Evaluation and Certification Guidance (May. 21, 2005)
[6] Korea IT Security Evaluation and Certification Scheme (Dec. 26, 2005)
[7] VForce 2200 V1.0 Security Target V1.1(2006. 7. 20), Nexg Co., LTD
[8] VForce 2200 V1.0 Evaluation Technical Report, V1.1(Sept. 20 2006)