KECS-CR-05-22

# Certification Report V1.0 on SECUREWORKS IPSWall 1000 V4.0 of OULLIM Information Technology Inc.

Certification No. : KECS-NISS-0049-2006

Aug. 2006

National Intelligence Service

IT Security Certification Center

This document is the certification report on SECUREWORKS IPSWall V4.0 of OULLIM Information Technology Inc.

Certification Body

National Intelligence Service

Evaluation Body

Korea Information Security Agency

# Table of Contents

# 1. Overview

This report is for the certification body to describe the certification result, which inspects the results of the EAL 4 evaluation of SECUREWORKS IPSWall 1000 V4.0 with regard to the Common Criteria for Information Technology Security Evaluation (Notification No. 2005-25 of the Ministry of Information and Communication; 'CC' hereinafter).

The Korea Information Security Agency (KISA) has evaluated the SECUREWORKS IPSWall 1000 V4.0, and finished the evaluation on the 22th of Dec. 2005. 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 V2.2 part 2 and EAL4 of the CC V2.2 part 3 assurance requirements; thus, it is assigned the verdict 'pass' on the basis of the paragraph 175 of the CC V2.2 part 1. In addition, the TOE satisfies the Network Intrusion Prevention System Protection Profile V1.0 (May. 24, 2005)

SECUREWORKS IPSWall 1000 V4.0 (the TOE), developed by OULLIM Information Technology Inc., is an appliance equipment that provides the IPS, VPN and Network Intrusion prevention system functions. The TOE is installed on the single connection point that separates the external and internal network, and is able to be installed and administered through the CLI(Command Line Interface) or GUI(Graphic User Interface).

- Access control function using the packet filtering SFP
- DPI(Deep Packet Inspection) function
  - Pattern matching function by using the HOTLIST
  - Protocol Anomaly Detection function
  - Traffic Anomaly Detection function
- Integrity check function on executable files and configuration files
- Administrator identification & authentication function
- Security management & Audit record function

The security functions, provided by the TOE but not included in the evaluation scope, are as follows; for more detail, refer to the ST.

- Virtual Private Network(VPN) function
- Application gateway function
- Network Address Translation (NAT) function
- Backup and transmission function of statistical data and audit data
- Virus engine and DI rule update function
- SecureDNS function to provide the DNS service by separating the internal and external network
- DHCP function
- General user identification and authentication function
- High Availability(HA) function
- One-Time Password(OTP) function
- Load Balancing and QoS function

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. In this regard, the certification body has confirmed that the evaluation results assure 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 made by the evaluator are accurate and reasonable; thus, certified that each verdict on each work package of the evaluator is correct.

Certification Validity: The information contained in the certification report means neither the use of SECUREWORKS IPSWall 1000 V4.0 is approved nor its qualification is assured by any Government Agency of the Republic of Korea.

# 2. TOE Identification

The [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)<br>Korea IT Security Evaluation and Certification Scheme (2005. 5. 7) |
| **TOE** | SECUREWORKS IPSWall 1000 V4.0 |
| **Protection Profile** | Network Intrusion Prevention System PP V1.0 (2005. 5. 24) |
| **Security Target** | SECUREWORKS IPSWall 1000 V4.0 ST V1.18 (2005. 8. 19) |
| **ETR** | SECUREWORKS IPSWall 1000 V4.0 ETR, V 1.02 (2005. 12. 22) |
| **Evaluation Result** | Satisfies the CC V2.2 part 2<br>Satisfies the EAL 4 of the CC V2.2 part 3 assurance requirements |
| **Evaluation Criteria** | Common Criteria for Information Technology Security Evaluation (2005. 5. 21)<br>Final Interpretation (2005. 6) |
| **Evaluation Methodology** | Common Methodology for Informations Technology Security Evaluation V2.2<br>Final Interpretation (2005. 6) |
| **Sponsor** | OULLIM Information Technology Inc. |
| **Developer** | OULLIM Information Technology Inc. |
| **Evaluation Team** | KISA IT Security Evaluation Center, Evaluation Team I<br>Yongseok Oh, Yeowoong Yoon, Hyuncho Kwon, Eunkyeong Yi<br>Jinsu Hyun |
| **Certification Body** | National Intelligence Service |

The TOE is an appliance that requires the system specification as stated in the [Table 2].

[Table 2] SECUREWORKS IPSWall 1000 V4.0 System Specification

| | | |
|---|---|---|
| CPU | | Celeron 2.6GHz |
| Flash RAM | | 128MB |
| RAM | | DDR 512MB |
| HDD | | Larger than 3.5 inch HDD PATA type 80GB |
| Interface | Network | 10/100 Fast Ethernet 4 |
| | Administration | DB9 + 1cDB9(for modem) |
| Chipset | | 845 GV+Winbond 83627 HF, Cavium Nitrox CN1005i |
| PCI Slot | | 64 Bit/66 Mhz PCI Slot |
| Power Supply | | Single Free Voltage |
| O/S | | SWOS V4.0 (Dedicated O/S) |

# 3. Security Policy

The TOE operation conforms to the security policies stated below.

### Packet filtering

The TOE admits the network traffic in case there is any access control rule which is clearly set as 'Admit' and denies it in the other cases using the source and destination addresses, service, port and the security attributes of the interface. There are additional security policies such as administrator multiple access, session termination, SSL channel, etc.

### Intrusion Prevention

Checks the attack pattern rule and protocol using the packet header information such as IP, TCP, UDP and ICMP and blocks the packets which are judged as attack. Terminates the corresponding session if it exceeds the session number specified by an authorized administrator.

### Identification & Authentication

An administrator should pass through the process of identification and authentication before using the security function of the TOE.

### TSF Protection

Should periodically inspect whether they are illegitimately modified using the integrity check function for such important files as the executable file of the TOE and the configuration file. Should detect failures such as a network communication failure, discontinuity of daemons, a buffer overflow, etc. and counter them.

### Security Management

Only an authorized administrator who accesses through trusted communication can the security management function.

### Security Audit

Security related events must be recorded and saved to be able to trace the responsibility of all actions, and the recorded data must be reviewed. The audit storage capacity should be administrated to keep recording the audit data.

# 4. TOE Assumptions & Scope

## 4.1 Assumptions

The TOE installation and operation should conform to the assumptions stated next.

### A.Attack Level

The attacker possesses a medium level of expertise, resources, and motivation. Chances of the attacker finding an exploitable vulnerability are moderate.

### A.Physical Security

The TOE is located in physically secure environment where only authorized administrators are allowed the access.

A.Security Maintenance

When the internal network environment is changed due to network configuration changes, an increase or decrease of hosts, or an increase or decrease of services, the new changes are immediately noted and security policies are configured in accordance with the TOE operational policy to maintain the same level of security as before.

A.Trusted Administrator

An authorized administrator of the TOE possesses no malicious intention, is adequately educated, and performs his/her duties in accordance with the administrative guideline.

A.Hardened OS

The underlying OS of the TOE ensures the reliability and stability by both eliminating unnecessary services or means not required by the TOE and installing the OS patches.

A.Single Connection Point

The TOE is installed and operated on a network and separates the network into external and internal network. Information can not flow between the two without passing through the TOE.

A.Secure TOE External Server

The network time protocol (NTP) server which maintains a trusted time outside the TOE for functions of the TOE and the DI rule update server which updates the latest DI rules are secure. The TOE uses the SSL protocol to create secure channels with the remote administrator PC and the DI rule update server.

A.SSL Certificate of the TOE

SECUREWORKS issues the certificate to be used for an SSL authentication in advance at installation and saves it in the TOE. The SSL certificate of the TOE is issued and controlled in a secure manner.

## 4.2 Scope to counter a threat

The TOE provides a means to counter a security threat, appropriate for the IT environment required rigourous control for the network traffic. Although the TOE does not have a counter-measure for a direct physical attack that makes the

SFP ineffective or bypasses, it provides a means to counter threat agents possessing medium-level expertise, resources, and motivation. In addition, it provides a counter-measure for a service attack/abnormal packet attack that disguises as an authorized administrator to access the TOE or exhaust the audit storage. An attack is not able to bypass the SFPs provided by the TOE, for it counters continuous authentication attempts and has a means to counter unauthorized modification of the TSF data.

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

# 5. TOE Information

The TOE provides the intrusion prevention system; consists of the following major subsystems.

- Security Management(AS)

  Performs the administrator authentication, integrity check, TOE configuration setup for an authorized administrator to define the TOE security policies and protect the TOE function. Displays the log data DB for the administrator to search the audit data generated in the TOE.

- Log management(LS)

  Creates and stores audit records of security related events occurred while enforcing security functions, and alarms the administrator for important audit data. Audit data generated in the CE subsystem is saved in the buffer managed by the core engine system, which gets to be stored in the DB through the log management subsystem. The information to generate the audit data occurred in the AS and SS subsystem is transmitted to the LS subsystem, so that the LS records and stores it.

- Core Engine(CE)

  Applies SFPs-packet filtering, intrusion prevention- to a packet passing through the network interface. The SFPs can allow/deny a packet or apply the deep packet inspection policy to it, based on the core engine subsystem. Each SFP consists of the network interface, source/destination address, service rules. A packet arrived through the network interface has to enters into the core engine subsystem without

exception. The subsystem applies the deep packet inspection policy to the allowed packet, and forwards a secure packet, ensured by the protocol check and attack pattern matching, to the final destination.

• Service Support(SS)

Service support component performs network related functions of the TOE such as network interface state testing.

# 6. Guidance

The TOE provides the following guidances:

- SECUREWORKS IPSWall 1000 V4.0 Installation Guidance Version 1.21, Aug. 26, 2005
- SECUREWORKS IPSWall 1000 V4.0 Administrator Guidance Version 1.23, Aug. 26, 2005
- SECUREWORKS IPSWall 1000 V4.0 Delivery Documents Version 1.3, Aug. 30, 2005
- SECUREWORKS IPSWall 1000 V4.0 Operation Guidance Version 1.14, Aug. 18, 2005

# 7. TOE Test

## 7.1 Developer's Test

• Test Method

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

- Testing No./Tester : The identifier of the test and the developer who participated in testing
- Purpose of the test : Describe the purpose of the test including security function of test subject and security module
- Test configuration : Detailed test configuration to carry out the testing
- Detailed test procedure : Detailed procedure to test security functions
- Expected result : The expected test result when implementing test procedure
- Actual result : The test result when implementing actual test procedure

- Comparison of the expected result and the actual result : The result of comparison of the expected result and the actual result

The evaluator evaluated the reasonability of the testing such as the test configuration, test procedure, analysis of test scope and the test of low-level design. The developer 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, PC and the server. In addition, it describes detailed test configuration such as the application sever(web server, mail server and etc.) required for test and test tools.

• Test scope analysis/Low-level design test

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

• Test Result

The test documentation describes the expected result and the actual result of each test. The actual result is confirmed through not only GUI of the TOE but the audit record.

## 7.2 Evaluator's Test

The evaluator installed the TOE by using the evaluation configuration and evaluation tools identical to the developer test, and examined the overall tests provided by the developer. The evaluator assured that the actual test result is consistent with the expected result.

Moreover, the evaluator devised evaluator tests additionally on the basis of developer test, and confirmed that the actual test result is consistent with the expected test result.

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

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

# 8. Evaluation 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: 6 sets (6 computer sets for the internal and external Computer)
- CPU: More than 600MHz
- RAM: More than 256MB
- Hard disk: More than 10GB

The following software is used for the evaluation configuration;

- Hancom Linux 3.1
- Windows 2000 server

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

# 9. Evaluation Result

The evaluation is on the basis of the final interpretation (as of 4th of July, 2005) of the Common Criteria for Information Technology Security Evaluation and Common Methodology for Informations Technology Security Evaluation V2.2. It concludes that the TOE satisfies the CC V2.2 part 2 and EAL4 of the CC V2.2 part3 assurance requirements. The detail information regarding the evaluation is described in the ETR.

• ST evaluation (ASE)

The evaluator applied the ASE sub-activities described in the CC V2.2 to the evaluation of the ST of the TOE.

The ST introduction is complete and consistent with all parts of the ST, and correctly identifies the ST.
The TOE description contains relevant information to aid the understanding of the purpose of the TOE and its functionality, and is complete and consistent

The statement of TOE security environment in the ST 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 they counter the identified threats, achieve the identified organisational security policies and are consistent with the stated assumptions.
The TOE security requirements (both the TOE security functional requirements and the TOE security assurance 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 instantiation of any PP for which compliance is being claimed.

Thus, the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding the TOE evaluation.

• Configuration Management Evaluation (ACM)

The evaluator applied the ACM sub-activities described in the CC V2.2 to the evaluation of the configuration management of the TOE.

From configuration management documentation, it is confirmed that the developer controls changes to the implementation representation with the support of automated tools.
From configuration management documentation, it is confirmed that the developer has clearly identified the TOE and its associated configuration items, and whether the ability to modify these items is properly controlled3.
From configuration management documentation, it is confirmed that the developer performs configuration management on the TOE implementation representation, the evaluation evidence required by the assurance components in the ST and security flaws.
Thus, configuration management documentation assists the consumer in identifying the evaluated TOE and ensures that configuration items are uniquely identified, and the adequacy of the procedures that are used by the developer to control and track changes that are made to the TOE.

• Delivery and Operation Evaluation(ADO)

The evaluator applied the ADO sub-activities described in the CC V2.2 to the evaluation of the delivery and operation of the TOE.

The delivery documentation describes all procedures used to maintain security and detect modification or substitution of the TOE when distributing the TOE to the user's site.

The procedures and steps for the secure installation, generation, and start-up of the TOE have been documented and result in a secure configuration.

Thus, the delivery and operation documentation used is adequate to ensure that the TOE is installed, generated, and started in the same way the developer intended it to be and that it is delivered without modification.

• Development Evaluation (ADV)

The evaluator applied the ADV sub-activities described in the CC V2.2 to the evaluation of the development of the TOE.

The functional specification describes all security functions of the TOE adequately and the security functions provided by the TOE are sufficient to satisfy the security functional requirements of the ST.
The security policy modeling clearly and consistently describes the rules and characteristics of the security policies; and this description corresponds with the description of security functions in the functional specification.
The high-level desing provides a description of the TSF in terms of major structural units, provides a description of the interfaces to these structural units, and is a correct realisation of the functional specification.
The low-level desing describes the interrelationship and dependencies between the modules with regard to the internal operation of the TOE security functions. The low-level design is sufficient to satisfy the functional requirements of the ST, and is a correct and effective refinement of the high-level design.
The implementation representation is sufficient to satisfy the functional requirements of the ST and is a correct realisation of the low-level

design.
The representation correspondence shows the developer has correctly and completely implemented the requirements of the ST, the functional specification, the high-level design and the low-level design in the implementation representation.

Thus, the following design documentation is adequate to understand how the TSF provides the security functions of the TOE; the functional specification which describes the external interfaces of the TOE, high-level design which describes the architecture of the TOE in terms of internal subsystems, low-level design which describes the architecture of the TOE in terms of internal modules, implementation representation of the source code level description, and the representation correspondence which maps representations of the TOE to one another in order to ensure consistency.

• Guidance Evaluation (AGD)

The evaluator applied the AGD sub-activities described in the CC V2.2 to the evaluation of the guidance of the TOE.

The administrator guidance describes how to administer the TOE in a secure manner.

Thus, the guidance document adequately describes how to administer and use the TOE in a secure manner.

• Life Cycle Support Evaluation (ALC)

The evaluator applied the ALC sub-activities described in the CC V2.2 to the evaluation of the life cycle support of the TOE.

It is confirmed that the developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised.
It is confirmed that the developer has used a documented model of the TOE life-cycle.
It is confirmed that the developer has used well-defined development tools that yield consistent and predictable results.

Thus, the procedures the developer uses during the development and maintenance of the TOE are adequately described; these procedures include the security measures used throughout TOE development, the life-cycle model used by the developer, and the tools used by the developer throughout the life-cycle of the TOE.

• Tests Evaluation (ATE)

The evaluator applied the ATE sub-activities described in the CC V2.2 to the evaluation of the test of the TOE.

The testing is sufficient to establish that the TSF has been systematically tested against the functional specification.
The developer has tested the TSF against its high-level design.
The developer's functional test documentation is sufficient to demonstrate that security functions perform as specified.
By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified, and to gain confidence in the developer's test results by performing entire developer's tests.

Thus, by independently testing a subset of the TSF, it is confirmed that TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST.

• Vulnerability Assessment Evaluation(AVA)

The evaluator applied the AVA sub-activities described in the CC V2.2 to the evaluation of the vulnerability assessment of the TOE.

From the misuse analysis, it is confirmed that the guidance is not misleading, unreasonable or conflicting; secure procedures for all modes of operation have been addressed; and use of the guidance will facilitate prevention and detection of insecure TOE states1.
SOF claims are made in the ST for all probabilistic or permutational mechanisms; and the developer's SOF claims made in the ST are supported by an analysis that is correct.
The vulnerability analysis document describes that appropriate measures are in place to prevent the exploitation of obvious vulnerabilities in the intended environment or indicates the guidance for that; the evaluator has conducted the independent vulnerability analysis to confirm the accuracy of the vulnerability analysis document.

From vulnerability analysis, it is confirmed that the TOE, in its intended environment, has no vulnerability exploitable by attackers possessing low attack potential.

Thus it is confirmed that there is no existence and exploitability of flaws or weaknesses in the TOE in the intended environment, based upon analysis performed by the developer and the evaluator, and supported by evaluator testing.

# 10. Recommendations

- The TOE should be installed on separate network upon the initial installation, since basic configuration is possible in all of the hosts connected on the same network without any specific restriction on the additional configuration from remote administration host after set up the network interface.
- The TOE should provide the HOT LIST update function for detection rules against a new vulnerability, and the administrator shall remain the latest detection rules through regular update.
- The TOE should restrict the multiple connections of administrators. Meanwhile, security management may be impossible until session time-out, since it maintains the connected session in case of abnormal log-out. Thus, session time out of security management should be set up to be small and logged out normally.
- The TOE should provide the administrator alarm function when it reaches the threshold due to shortage of storage space of audit record, However, the administrator should not depend just on the alarm function, but check the usage of storage space continuously and secure storage space for audit record.

# 11. Acronyms and Glossary

The following acronyms are used in the certification report.

| | |
|---|---|
| CR | Certification Report |
| DI | Deep Inspection |
| EAL | Evaluation Assurance Level |
| IT | Information Technology |
| KECS | Korea IT security Evaluation and Certification Scheme |
| QoS | Quality of Service |
| TOE | Target of Evaluation |

The following terms are used as stated next, in the certification report.

**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 accordace 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

**Assets**

Information and resources to be protected by the countermeasures of a TOE

**Intrusion Prevention System**

IT product that is architected to instantaneously act on attack detection by automatically blocking malicious activity before damage occurs.

**Virus**

A program or piece of code that is located onto your computer without your knowledge and runs against your wishes

**Worm**

A special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

**Daemon**

A process that runs in the background and performs a specified operation at predefined times or in response to certain events

**NTP**

An internet standard protocol built on top of TCP/IP that assures accurate synchronization to the millisecond of computer clock times in a network of computers

**HOTLIST**

Database for maintenance of latest attack rules

**DI**

Rules containing type of attacks defined using pattern, level, services, data size, IP datagram, transport datagram, etc. to block abnormal packets and DOS attack

**DI Rule Update Server**

Server that updates latest attack rules, HOTLIST, to the TOE

**SWIP**

SECUREWORKS virtual IP driver that is core engine that performs major functions of IPS

# 12. Reference

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 V2.2
[3] Network Intrusion Prevention System Protection Profile V1.0 (May. 24, 2005)
[4] Korea IT Security Evaluation and Certification Guidance (May. 21, 2005)
[5] Korea IT Security Evaluation and Certification Scheme (May. 7, 2005)
[6] SECUREWORKS IPSWall 1000 V4.0 Security Target V1.18 (Aug. 19, 2005), OULLIM Information Technology Inc.
[7] SECUREWORKS IPSWall 1000 V4.0 Evaluation Technical Report, V1.0 (2005. 12. 22)