PREMIER MINISTRE

Secretariat General for National Defence

French Network and Information Security Agency

Certification report ANSSI-2009/30

IPS-Firewall software suite for NETASQ appliances version 8.0.1.1

Paris, 03 August 2009

Courtesy Translation

Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.
Certification does not, however, constitute a recommendation product from ANSSI (French Network and Information Security Agency), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

Secrétariat Général de la Défense Nationale
Agence nationale de la sécurité des systèmes d'information

Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.dcssi@sgdn.gouv.fr

Certification report reference

ANSSI-2009/30

Product name

IPS-Firewall software suite for NETASQ appliances

Product reference

Version 8.0.1.1

Protection profile conformity

None

Evaluation criteria and version

Common Criteria version 3.1

Evaluation level

EAL 4 augmented

ALC _FLR.3

Developer(s)

NETASQ

3 rue Archimède, 59650 Villeneuve d'Ascq, France

Sponsor

NETASQ

3 rue Archimède, 59650 Villeneuve d'Ascq, France

Evaluation facility

Silicomp-AQL

1 rue de la châtaigneraie, CS 51766, 35513 Cesson Sévigné Cedex, France

Phone: +33 (0)2 99 12 50 00, email : cesti@aql.fr

Recognition arrangements

CCRA **SOG-IS**

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The French Network and Information Security Agency draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the sponsors desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr.

Contents

1. The product

1.1. Presentation of the product

The evaluated product is the "IPS-Firewall software suite for NETASQ appliances, version 8.0.1.1" developed by NETASQ. The evaluation covers solely the filter function.

The IPS-Firewall software suite for NETASQ appliances offers firewall-type functions including network filtering, attack detection, bandwidth management, security policy management, audit, accountability and strong user authentication. It also proposes VPN (Virtual Private Network: encryption and authentication) functions that implement the ESP (Encapsulating Security Payload) protocol in IPSec standard tunnel mode, thereby securing the transmission of data between remote sites.

The IPS-Firewall software suite comprises the following components:

Component	TAG
IPS-Firewall	8.0.1.1
Administration suite (Manager, Reporter, Monitor)	8.0.1

This software suite, containing the filter function, was also evaluated and certified at level EAL3 augmented with additional components ALC_CMC.4, ALC_CMS.4, ALC_FLR.3 and AVA_VAN.3 under the reference ANSSI-2009/29 [2009_29] on 29 July 2009.

1.2. Description of the product

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operational environment.

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.

A label attached to the appliance packaging indicates the version of the software installed on the firewall.

If you install and connect using the Firewall Manager application provided on the CD-ROM, the Manager application displays the model, serial number and appliance version on the screen. The administration software displays the installed software version on the main window and in the "Help" menu.

1.2.2. Security services

The security services provided by the target of evaluation are:

- filtering of data flows between equipments;
- generation of audit data.

1.2.3. Architecture

The **IPS-Firewall** (also referred to as **NS-BSD**) runs on an appliance connected to a remote administration workstation (where the administration suite runs) via a network connection.

The Target of Evaluation (TOE) is a component of the part of the software suite installed on the Firewall-VPN appliance. The diagram below describes the TOE in its environment.
The software suite comprises the following components:

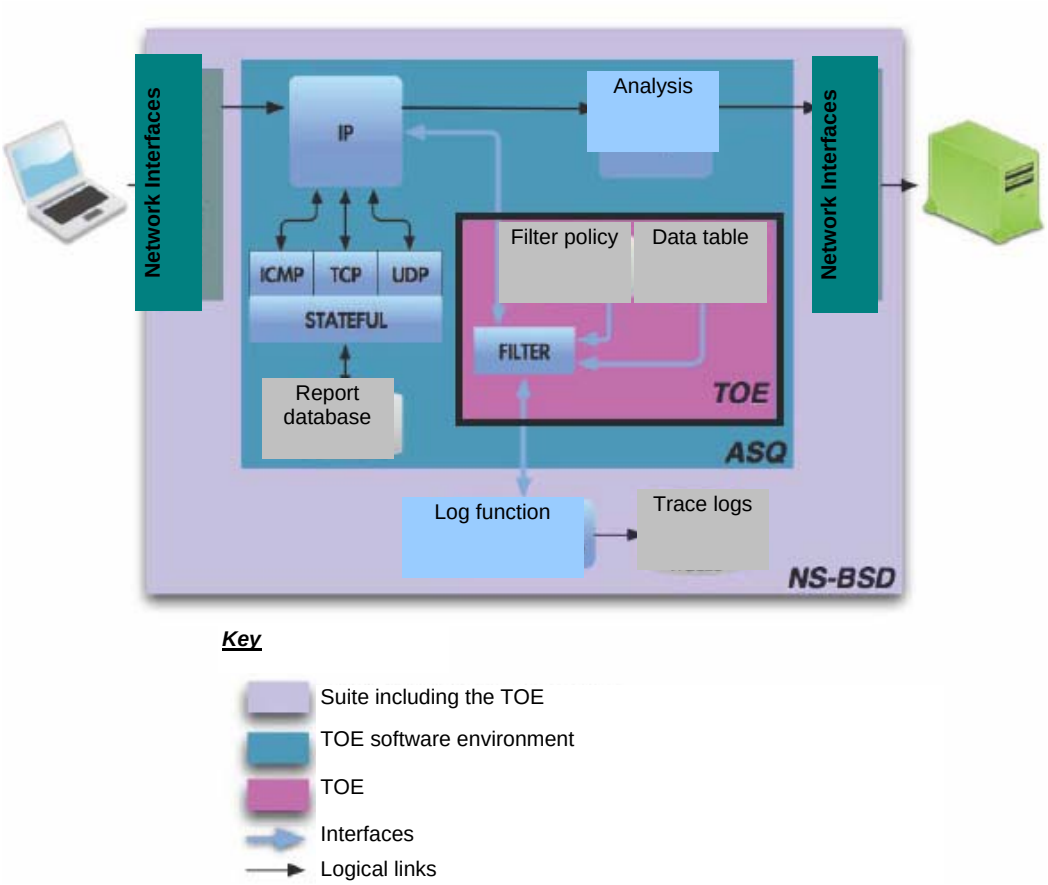

Figure 1 - TOE Architecture

The evaluation concerned the filter function "**Filter"** of the ASQ (Active Security Qualification) module of the IPS-Firewall software.

ASQ is a Real-Time Intrusion Prevention technology, integrated in all NETASQ IPS-Firewalls.

1.2.4. Life cycle

The product's life cycle is organised as follow:

- **Development**: development of the software suite;
- **Deployment**: provision of the software suite to clients (CD-ROM for the administration suite and appliance for the IPS-Firewall software);
- **Installation**: installation of the software according to the guidance provided [GUIDES]

- **Operations and Maintenance**: day-to-day monitoring, bug reports if required;
- **Scrapping:** destruction of obsolete or defective product.

Only the development and deployment phases (performed by NETASQ) were evaluated.

The installation, operations and scrapping phases were performed by the client.

The IPS-Firewall software suite was developed on the site indicated below:

NETASQ

3 rue Archimède
59650 Villeneuve d'Ascq
France

In the evaluation context, the persons performing security administration operations and responsible for their completion in accordance with guidance [GUIDES] have been considered as "product administrator" and the persons using trusted network resources protected by the product via other trusted networks or from non-managed networks have been considered as "product user".

The "super-administrator" is in charge of defining administrator profiles. This person only intervenes during the installation phase and maintenance activities. He alone is permitted to connect to the appliances via the local console and must have sole authority to grant access to the appliance storage room.

1.2.5. Evaluated configuration

The evaluation concerned the filter function of the IPS-Firewall software suite version 8.0.1.1 running on the F200 and U250 models of the Firewall-VPN appliance.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1** [CC] and with the Common Evaluation Methodology [CEM].

2.2. Evaluation work

The evaluation technical report [ETR], delivered to ANSSI the 24 July 2009, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis

The target of evaluation does not use cryptographic mechanisms. Their robustness was not therefore analysed by ANSSI.

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality of a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the product “IPS-Firewall software suite for NETASQ appliances version 8.0.1.1” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 augmented.

3.2. Restrictions

This certificate only applies on the product specified in chapter 1.2 of this certification report.

The user of the certified product shall respect the security objectives for the operational environment specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:

- the appliances must be installed and stored using state of the art methods for sensitive security devices;
- the appliances must be installed to be the exclusive points of interconnection between the networks where the information flow control policy must be applied;
- the filter policy must be defined, for all equipment on the trusted networks to be protected, fully, strictly, correctly and unambiguously;
- administrators must be trustworthy, skilled and correctly trained, with the necessary resources to accomplish their responsibilities;
- product administrators must protect login information and passwords in the Manager software by encrypting the user directory;
- other than the security functions, the appliances must not provide network services apart from routing and address translation;
- the IPS-Firewall software suite must provide the filter function with a secure log service which formats, timestamps and records audit data.

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is released in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[2], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.

2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

Annex 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3 +	Name of the component
ADV Development	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic modular design
AGD Guidance	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance, procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	Development tools CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined developments tools
ASE Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	**2**	**3**	3	**4**	**2**	Testing: security enforcing modules
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**3**	Focused vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for evaluation: - Firewalls NETASQ – Cible de sécurité Fonction de filtrage de la suite logicielle IPS-Firewall Version 8 Reference: NA_ASE_ciblesec_filter, version 1.3 dated 27/03/2009 NETASQ
[ETR]	Technical evaluation report : Rapport technique d'évaluation – Projet SANDRINE Reference: NTQ004-Sandrine-ETR, version 4.01 dated 24/07/2009 Silicomp AQL
[CONF]	Configuration list Reference: NA_ALC_sources_liste_v8, version 1.0 dated 12/01/ 2009 NETASQ
[2009_29]	Certification Report ANSSI-2009-29 – "Suite Logicielle IPS-Firewall pour boîtiers appliances NETASQ" 29 July 2009 SGDN/ANSSI
[GUIDES]	Manager interface user guide: - NETASQ UNIFIED MANAGER V8.0 – Manuel d'utilisation et de configuration Reference: FRUG0907-V1.2_NUMANAGER-V8.0, version 1.2 dated July 2009 NETASQ Monitor interface user guide: - NETASQ REAL-TIME MANAGER V8.0 – Manuel d'utilisation et de configuration Reference: FRUG0901-V1.1_NRMONITOR-V8.0, version 1.1 dated January 2009 NETASQ Reporter interface user guide: - NETASQ EVENT REPORTER V8.0 –Manuel d'utilisation et de configuration Reference: FRUG0901-V1.1_NEREPORTER-V8.0, version 1.1 dated January 2009 NETASQ

Annex 3. Certification references

Decree number 2002-535 dated 18th April 2002 related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 - Certification of the security provided by IT products and systems, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.