PREMIER MINISTRE

Secretariat General for National Defence

French Network and Information Security Agency

Certification Report ANSSI-2009/29

IPS-Firewall software suite for NETASQ appliances, version 8.0.1.1

Paris, 29 July 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-2009/29

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 3 augmented

ALC_CMC.4, ALC_CMS.4, ALC_FLR.3, AVA_VAN.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 « IPS-Firewall software suite for NETASQ appliances**,** Version 8.0.1.1 » developed by NETASQ.

This product offers firewall-type functions including network filtering, attacks detection, bandwidth management, security policy management, audit, accountability and strong user authentication. It also provides VPN (Virtual Private Network: encryption and authentication) functions which use the ESP (Encapsulating Security Payload) protocol in IPSec standard tunnel mode to secure the transmission of data between remote sites.

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 each appliance, indicates the model, serial number, client web activation code and also a barcode of the serial number.

Another label, attached to the packaging containing the appliance and the administration software CD-ROM, displays the version of the software installed on the appliance.

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 main security services provided by the product are:

- filtering data flows between equipment;
- user identification and authentication;
- encryption (for VPN);
- establishment of security associations (SA);
- logs, audits and alarms;
- intrusion prevention;
- access control to security administration operations;
- backups and restorations;
- protection of administration sessions.

1.2.3. Architecture

The software suite is made up of the following software parts:

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

The **IPS-Firewall** runs on an appliance connected to the remote administration workstation. Through a network

The **NETASQ Administration Suite (GUI)** package, which runs on the administration workstation, has three graphical user interfaces:

- **NETASQ Unified Manager**, which allows the NETASQ firewalls administration and configuration;
- **NETASQ Real-Time Monitor**, which allows supervision and monitoring of one or more firewalls;
- **NETASQ Event Reporter**, which allows trace analysis and reporting.

1.2.4. Life cycle

The product's life cycle is organised as follow:

- **Development**: development of the target of evaluation (TOE);
- **Deployment**: provision of product to clients;
- **Installation**: compliance with NETASQ recommendations;
- **Operations**: day-to-day production monitoring, bug reporting if required;
- **Scrapping**: destruction of obsolete or defective products.

Only the development and deployment phases (performed by NETASQ) were evaluated.
The installation, operations and scrapping phases were performed by the client.

The product has been developed on the following site:

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 defininig administrator profiles. This person only intervenes during the installation phase and maintenance activities. He alone is permetted 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 evaluated configuration corresponds to:

- IPS-Firewall software version 8.0.1.1 run on the F200 and U250 models of the Firewall-VPN appliance;
- NETASQ administration suite version 8.0.1 installed on a workstation with Windows XP SP3.

The constituent elements of the target of evaluation are indicated on the diagram below, along with the full test platform deployed by the developer:

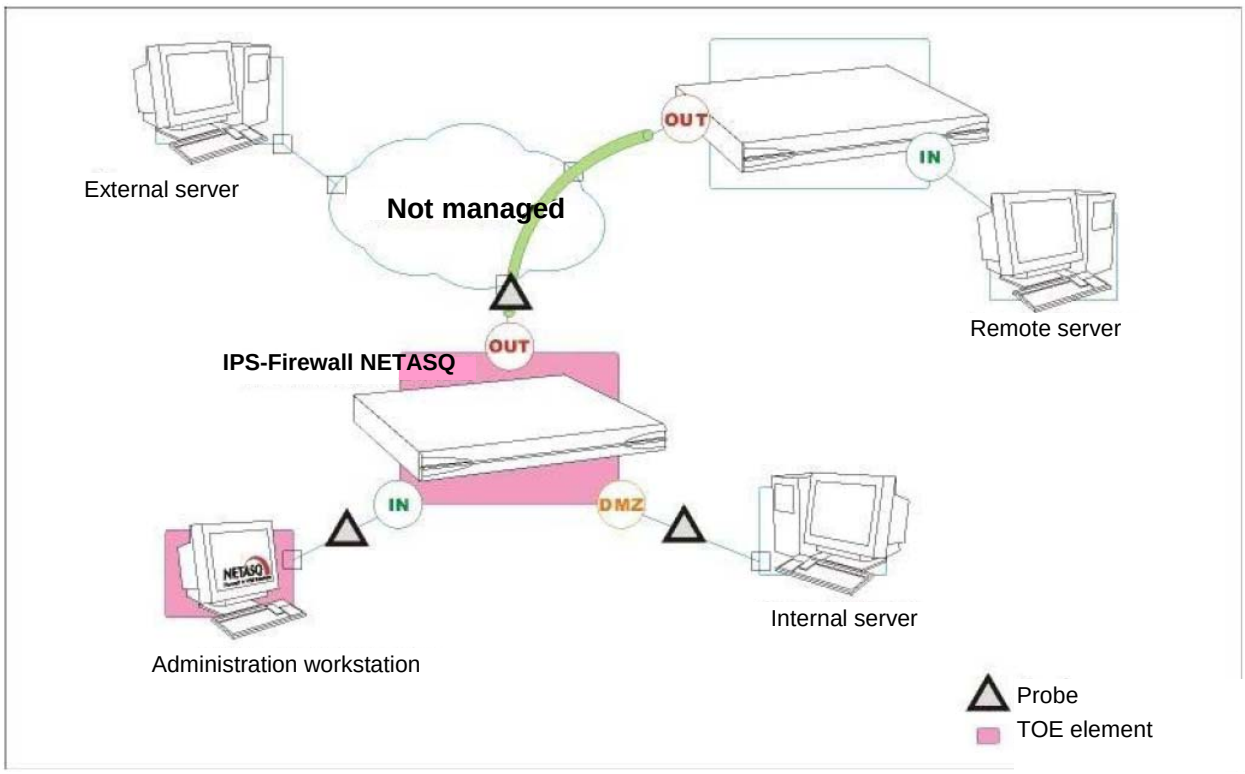

Figure 1 – Constituent elements of theTarget of Evaluation

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 robustness of cryptographic mechanisms has been analysed by ANSSI. The results are stated in the cryptographic analysis report [ANA-CRY]. The analysed mechanisms reach the standard robustness level defined in the ANSSI cryptographic referential (Cf. [REF-CRY]).

In the context of standard qualification process, an analysis of the cryptographic mechanisms was performed by the ITSEF [EXP-CRY]. These results were included in the independent vulnerability analysis performed by the evaluator and did not result in the detection of an exploitable vulnerability for the AVA_VAN level in question.

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 3 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 follow 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 data flow security policy must be applied;
- the network equipment used by the product to establish the VPN tunnels must be protected to the same level as the appliances;
- the remote administration workstations must be secured, maintained up to date against all known vulnerabilities, and installed in restricted access premises. They must be used exclusively for the administration of the target of evaluation and for data storage;
- workstations where authorised users run VPN clients must be protected to the same level as the remote administration stations;
- user and administrator passwords must be managed through a password creation and verification policy;
- administrators must be trustworthy, skilled and correctly trained, with the necessary resources to accomplish their responsibilities;
- the super-administrator must be the only person authorised to connect to the appliances via the local console;
- the data flow security policy must be defined, for all equipment on the trusted networks to be protected, fully, strictly, correctly and unambiguously;
- the target of evaluation must not depend on external "online" services to apply the data flow security policy;
- other than the security functions, the appliances must not provide network services apart from routing and address translation;
- the cryptographic algorithms and key sizes corresponding to the options specified in the security target [ST chapter 5.2.5], listed in the table below, must be used (including the following modification: it is recommended to adopt at least 2048 bits key size for the Diffie-Hellman algorithm):

Cryptographic operation	*Algorithm*	*Key size*
Key establishment and signature	Diffie-Hellman	~~1536~~, 2048, 3072, 4096
Asymmetric encryption / decryption	RSA	2048, 4096
Univocal hashing	HMAC-SHA1	160
	SHA2	256, 384, 512
Symmetric encryption /decryption of VPN packets	AES	128, 192, 256
	Triple DES	168
	Blowfish	128 to 256
	CAST	128
Symmetric encryption /decryption of administration sessions	AES	128
Administration session security	HMAC-SHA1	160

The certified product administrator must also respect the following recommendations:

- protect login information and passwords in the Manager software by encrypting the user directory;
- systematically activate integrity protection on IPSec flows;
- use HMAC-SHA1 integrity protection on IPSec flows;
- use authentication methods (pre-shared keys, public keys) according to rules and recommendations of [REF-CRY] for the key exchange authentication when executing the IKE (Internet Key Exchange) protocol.

If an external LDAP directory is used for user authentication, the remote server hosting the LDAP directory must be protected to industry-best standards. More precisely, one will seek to:

- use the SSL protocol to encrypt communications between the LDAP directory and the IPS-Firewall to ensure the confidentiality of information transported by the LDAP protocol. The external LDAP server must listen on port TCP 636 (default port for LDAP communications);
- create a specific administrator account enabling the IPS-Firewall to connect to the external LDAP server while restricting read/write capabilities to the fields required by the IPS-Firewall;
- select a hashing algorithm according to [REF-CRY] rules and recommendations on stored passwords.

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**	**3**	Functional specification with complete summary
	ADV_IMP				**1**	1	**2**	2		
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**2**	Architectural 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		
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**	**1**	Testing: basic design
	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 the evaluation: - NETASQ Firewalls – Cible de sécurité Suite logicielle IPS-Firewall Version 8 suite Reference: NA_ASE_ciblesec_v8, version 1.4 dated 15 April 2009 NETASQ
[ETR]	Evaluation technical report: Rapport technique d'évaluation – Projet JOCELYNE Reference: NTQ004-Jocelyne- ETR, version 4.01 dated 24 July 2009 Silicomp-AQL
[ANA-CRY]	Assessment of cryptographic mechanisms: Cotation de mécanismes cryptographiques – Projet JOCELYNE Reference: 1644/SGDN/DCSSI/ACE dated 26 June 2009 SGDN/DCSSI
[EXP-CRY]	Analysis of cryptographic mechanisms: Analyse des mécanismes cryptographiques – Projet JOCELYNE Reference NTQ004-AMC, version 1.02 dated 24 July 2009 Silicomp-AQL
[CONF]	Configuration list Reference: NA_ALC_sources_liste_v8, version 1.0 dated 12 January 2009 NETASQ
[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, revision 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.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard – Version 1.11 du 24 octobre 2008