Swedish Certification Body for IT Security

Certification Report - Firewall Protection Profile and Firewall Protection Profile Extended Package: NAT

Issue: 2.0, 2015-jun-12

Authorisation: Martin Bergling, Technical Manager , CSEC

Report Distribution: Anders Staaf, Combitech AB
Arkiv

Table of Contents

1 Executive Summary

This certification concerns one Protection Profile and one extended package:

- Firewall Protection Profile [PP3]
- Firewall Protection Profile, Extended Package: NAT [NAT3]

The TOE described in this protection profile is a firewall including network address translation, NAT.

The TOE is intended for use by organizations that need controlled, protected and audited access to services, both from inside and outside their organization's network.

The administrators of the TOE are assumed to be trained and trusted, and the TOE shall operate in a physically protected environment.

Attackers are either unauthorized persons or IT entities on the external network, or users on the internal network trying to undetected transmitting information or access services on the external network. The attackers are assumed to have no physical access, but unlimited network access (inside and outside) and time available.

The TOE described in this protection profile has several security functions: Information flow control, Management of the TOE, Administrator identification and authentication, Audit, Verification of software updates and Self-test and protection of system files, see section 3 below for more information.

The TOE must also provide at least one of two conditional security functionalities:

- Stateful Packet Filter (SPF)
- Deep Packet Inspection (DPI).

The extended package defined in [NAT3] also requires the TOE to perform Network Address Translation (NAT) or Port Address Translation (PAT).

Three security policies are defined, regarding administration of the TOE and regarding hiding of IPv4-addresses, see section 3 below for more information.

Six environmental assumptions are defined, regarding the location of the TOE, the physical environment, the underlying hardware, safe storage of audit trails, non-hostile administrators and reliable time, see section 4.2 below for more information.

The assurance package is EAL2 augmented with ALC_FLR.1 (basic flaw remediation).

- EAL2 is applicable in those circumstances where users require a low to moderate level of independently assured security.
- The augmentation ALC_FLR.1 is chosen to ensure that basic flaw remediation is in place.

The Protection Profile, including the Extended Package NAT, is aiming to be covered under the CCRA Mutual Recognition Agreement [CCRA].

The evaluation was conducted by Combitech AB, a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The evaluation was performed according to the APE requirements in Common Criteria version 3.1 [CC], and Common Methodology for Information Technology Security Evaluation, version 3.1, [CEM].

The evaluation completed with PASS on all work units and with no remaining potential or residual vulnerabilities identified.

The author of the protection profiles is atsec information security AB.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results have been reached in accordance with the requirements of the Common Criteria and the Common Methodology.

The certificate applies only to the specific version and release of the protection profile listed in this certification report.

The certificate is not an endorsement of the protection profile by CSEC or by any other organisation that recognises or gives effect to this certificate, and no warranty of the protection profile by CSEC or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2014010
Name and version of the certified Protection Profile	Firewall Protection Profile, 2015-03-12, No. 2014-701, version 3.0 Firewall Protection Profile, Extended Package: NAT, 2015-03-12, No. 2014-701, version 3.0
EAL	EAL 2 + ALC_FLR.1
Sponsor	Combitech AB
Developer	atsec information security AB
ITSEF	Combitech AB
Common Criteria version	3.1 release 4
CEM version	3.1 release 4
National and international interpretations	-
Recognition Scope	CCRA MRA, SOGIS-MRA, EA MLA
Certification date	2015-06-12

3 Security Policy

The following Organisational Security Policies are defined:

- P.MANAGE - The TOE shall support the means to administrators to manage the security functions. The management may be performed locally at the TOE, remotely from a separate management network or from the internal network.
- P.ADMACC - Administrators shall be held accountable for their actions through audit records.
- P.HIDE_NAT - The TOE shall be able to hide the IPv4 addresses of the entire IPv4 address space of the internal network.

The TOE, described in the protection profile, provides the following security functions:

- Information flow control - Information flow control (layer 3 and 4) between the external and the internal networks.
- Management of the TOE - Local and/or remote administration, configuration changes and software updates.
- Administrator identification and authentication - The remote administrators must be identified and authenticated by the TOE.
- Audit - Audit of security relevant events, trusted updates, configuration changes and self-tests.
- Verification of software updates - The TOE may perform software updates when initiated by an administrator. The TOE must verify the authenticity and integrity of the software and also verify that the software is newer that the current version before the TOE is using the new software.
- Self-test and protection of system files - Self-test and integrity verification of system files must be performed during start-up as well as initiated by the administrator.

The TOE claiming compliance to this Protection Profile must provide at least one of two conditional security functionalities:

- Stateful Packet Filter (SPF) - The Stateful Packet Filter (SPF) describes the security requirements for a packet filtering firewall that is capable of tracking information flow states.
- Deep Package Inspection (DPI) - The Deep Packet Inspection (DPI) describes the security requirements for a protocol aware filtering firewall, typically at layer 7 (e.g., HTTP).

The firewall may have optional functionality that may described in extended packages or claimed by the ST author directly in the ST. There is one extended package [NAT3] defined for the TOE in this certification:

- Network Address Translation (NAT) or Port Address Translation (PAT) - This means that the firewall will translate the network addresses or port numbers as part of its firewall functionality.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The TOE, described in the protection profile, is intended for use by organizations that need controlled, protected and audited access to services, both from inside and outside their organization's network. The TOE is intended to be located between the internal and external network, such as a local area network and the Internet, and shall mediate traffic according to information flow control policies. It is assumed to be the only connection between these two networks.

The administrators of the TOE are assumed to be trained and trusted in managing the TOE, as well as in general network management and network security. The TOE shall operate in a physically protected environment to ensure that the TOE cannot be physically accessed and tampered with.

4.2 Environmental Assumptions

The following assumptions on the operational environment are made:

- A.LOCATE - The TOE is located between an external network, and an internal network containing the User Data that is to be protected. It is the only point at which traffic can flow between the two networks.
- A.PHYSICAL - The TOE is operated in a physically secure environment, i.e., no unauthorized person has physical access to the TOE or its underlying software and hardware.
- A.RELHARD - The underlying hardware, software, firmware (BIOS and device drivers) and the operating system functions needed by the TOE to guarantee secure operation are working correctly, and have no undocumented security critical side effect on the security objectives of the TOE.
- A.AUDIT - The environment is able to receive, store and protect the audit records generated by the TOE and provides the means for analysis of the audit records.
- A.ADMIN - Authorized administrators given privileges to administrate the TOE are competent, non-hostile and follow all their guidance; however, they are capable of error.
- A.TIME - The TOE environment provides the TOE with a reliable time stamp.

4.3 Clarification of Scope

Usually perimeter protection consists of a range of different security functionalities in addition to the address and port filtering, such as application level analysis and filtering, intrusion detection and prevention, use of authentication services, Virtual Private Networks, content analysis (malware analysis). Note that not all of these security features are considered part of this firewall security functionality and only some of these features are part of this protection profile.

5 Architectural Information

There are at least two types of network interfaces of the firewall, the network interface to external networks and the network interface to internal networks. They are distinctly separate and there is at least one interface of each type, but there may be multiple interfaces of each type.

There may be additional networks (not shown in the picture below) for remote administration and audit, and additional interfaces for local administration. But the protection profile make no requirements neither on availability or nature of any such interfaces.

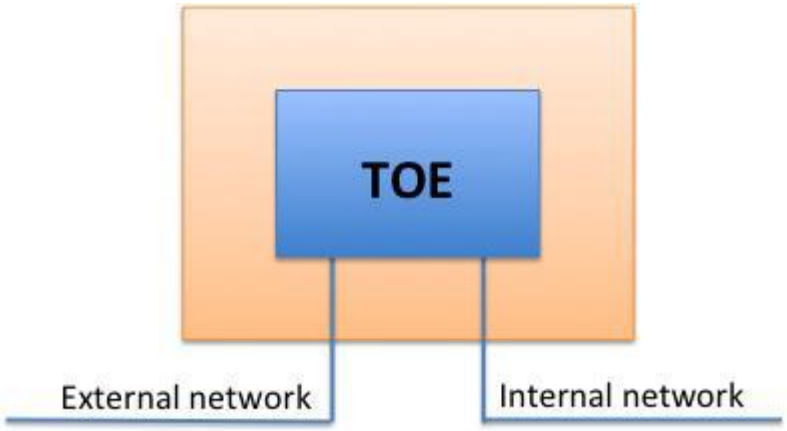

Figure 1: TOE scope and interfaces

The scope of the TOE require underlying software and hardware, which may include the operating system and hardware platform and network cards. The environment is able to receive, store and protect the audit records generated by the TOE and provides the means for analysis of the audit records.

The TOE environment provides the TOE with a reliable time stamp, which typically in a network environment is an NTP source that is trusted, typically located in the internal network.

The TOE requires functionality to process X.509 certificates.

6 Results of the Evaluation

The verdicts for the assurance classes and components are summarised in the following table. Summarizing the results of all assurance components, the final evaluation result is PASS.

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Protection Profile Evaluation	APE	Pass
PP Introduction	APE_INT.1	Pass
Conformance claims	APE_CCL.1	Pass
Security problem definition	APE_SPD.1	Pass
Security objectives	APE_OBJ.2	Pass
Extended components definition	APE_ECD.1	Pass
Security requirements	APE_REQ.2	Pass

7 Evaluator Comments and Recommendations

None.

8 Glossary and abbreviations

EA MLA	European Cooperation for Accreditation, Multilateral Arrangement
ITSEF	IT Security Evaluation Facility
NTP	Network Time Protocol
PP	Protection Profile
SOGIS-MRA	Senior Officers Group for Information Systems, Mutual Recognition Agreement
TOE	Target of Evaluation

Augmentation	The addition of one or more requirement(s) to a package.
Authentication data	Information used to verify the claimed identity of a user.
Authorised user	A user who may, in accordance with the SFRs, perform an operation.
Class	A grouping of CC families that share a common focus.
Component	The smallest selectable set of elements on which requirements may be based.
Evaluation	Assessment of a PP, an ST or a TOE, against defined criteria.
Evaluation Assurance Level (EAL)	An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.
Family	A grouping of components that share a similar goal but may differ in emphasis or rigour.
Guidance documentation	Documentation that describes the delivery, preparation, operation, management and/or use of the TOE.
Network Address Translation (NAT)	A mechanism for assigning local networks a set of IP addresses for internal traffic and another for external traffic. NAT was originally described in RFC 1631 as a means for solving the rapidly diminishing IP address space. It provides a supplemental security purpose by hiding internal IP addresses.
Operational environment	The environment in which the TOE is operated.
Organisational Security Policy (OSP)	A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment.
Package	A named set of either functional or assurance requirements (e.g. EAL 3).

Packet filter	A method of controlling access to a network, or set of networks, by examining packets for source and destination address information, and permitting those packets to pass, or halting them based on defined rules.
Port Address Translation (PAT)	A mechanism for reassigning port numbers used on the local connection to different port number on the external network assignment. It is often used in combination with Network Address Translation (NAT).
PP evaluation	Assessment of a PP against defined criteria.
Protection Profile (PP)	An implementation-independent statement of security needs for a TOE type.
Secure state	A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.
Security Function Policy (SFP)	A set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions.
Security Target (ST)	An implementation-dependent statement of security needs for a specific identified TOE.
ST evaluation	Assessment of an ST against defined criteria.
Target of Evaluation (TOE)	A set of software, firmware and/or hardware possibly accompanied by guidance.
TOE evaluation	Assessment of a TOE against defined criteria.
TOE Security Functionality (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

9 Bibliography

PP3	Firewall Protection Profile, 2015-03-12, No. 2014-701, version 3.0, 14FMV10188-27
NAT3	Firewall Protection Profile, Extended Package: NAT, 2015-03-12, No. 2014-701, version 3.0, 14FMV10188-28
CCRA	Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2, 2014
CC	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4, CCMB-2012-09-001/002/003
CEM	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1 Revision 4, CCMB-2012-09-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2014-12-12, document version 22.0, 14FMV9859-38:1

Appendix A Scheme Versions

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system. During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been applicable since the certification application was received 2014-11-13.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
1.16.2	2014-07-07	None.
1.17	2014-11-20	None.
1.17.1	2014-12-02	None.
1.17.2	2015-01-13	None.
1.17.3	2015-01-29	None.

The changes between consecutive versions are outlined in "Ändringslista QMS 1.17.3".

The certifier concluded that, from QMS 1.16.2 to the current QMS 1.17.3, there are no changes with impact on the result of the certification.