Myndigheten för samhällsskydd och beredskap

2015-03-12 2014-701 3.0

ROS-ISÄK
Ronny Janse
010-2404426
ronny.janse@msb.se

Firewall Protection Profile

Extended Package: NAT

Innehållsförteckning

1. Introduction

1.1 PP reference

Title:	Firewall Protection Profile: Extended Component – NAT/PAT
Version:	Release version 3.0, 2015-03-12
TOE Type:	IP Firewall
Evaluation Assurance Level:	EAL2 augmented with ALC_FLR.1
CC Version:	3.1 release 4
PP Author:	Staffan Persson Robert Hoffmann
Keywords:	Firewall, Extended Component, NAT, PAT, Address Translation, Port Translation

1.2 Overview

This Extended Package (EP) for NAT/PAT describes the security requirements for a packet filtering firewall that is capable of translating IP addresses between different networks.

The EP is not complete itself, but rather extends the Firewall Protection Profile (FPP) as an Extended Package.

NAT (Network Address Translation) is a technique to translate the IP addresses of hosts in one network into other addresses, when traversing the firewall.

PAT (Port Address Translation) is a NAT technique through which the IP addresses of 1..n “internal” hosts of one network are mapped onto one “public” IP address of a different interface of the firewall. This allows the hosts on the first network to share one address on another network. The typical use case is to allow multiple hosts on a private (internal) IP range to access the internet through one external public IP address.

For the TCP protocol, PAT is performed as follows: When an internal host opens a TCP connection to an external target, the firewall notes the source IP address and port of the connections and establishes a state. The packet source and port is then rewritten with the public IP of the firewall and a source port. As long as the state is established, any TCP packet arriving at the designated firewall public IP and port will be rewritten with the internal host’s target IP address and port, and routed to it.

UDP is by definition a stateless protocol. PAT for UDP is therefore implemented by observing the packet flow and handling expected packets similar to TCP. E.g., if an internal host sends a UDP packet to an external DNS server (query), the firewall expects a corresponding answer. The state is therefore established partly through expected protocol behavior.

PAT for ICMP is performed similar to UDP.

There exist further techniques to perform NAT, but for the scope of this EP the term NAT is defined by and limited to the PAT techniques and protocols as documented above.

1.2.1 Usage

Since this EP extends the FPP, a Security Target that claims compliance with this EP must also comply with the FPP.

NAT/PAT can be performed for various protocols and ISO/OSI layers. The protocols supported by this EP are exclusively IPv4, TCP, UDP and ICMP.

1.3 TOE description

1.3.1 Introduction

The basic TOE functionality and capabilities are describes in the FPP.

1.3.2 Intended usage

The intended usage of the TOE is described in the FPP.

1.3.3 Security features

This EP defines the following additional security functions, extending the FPP:

- Information flow control: Packet translation (NAT/PAT).

1.4 References

[FPP]	Firewall Protection Profile, MSB, 2015-03-12.

2. Conformance claims

This extended package does not augment the conformance claim of the FPP base package.

This extended package does not depend on other FPP extended packages.

This package can only be claimed together with the FPP base package in the version defined in [FPP].

This extended package does not conflict with any other FPP extended package available at the time of publication.

3. Security problem definition

The security problem definition of the FPP Extended Package – Network Address Translation extends the security problem definition of the FPP base, which defines the basic security requirements for a firewall.

The following sections provide a definition of various important terms, threats, assumptions and policies that are the basis for the security functionality of this FPP extended package.

3.1 Assets

The assets are consistent with the assets given in the FPP base.

3.2 Threat agents

The threat agents are consistent with the definition of threat agents given in the FPP base.

3.3 Threats

The threats are consistent with the definition of threat agents given in the FPP base.

3.4 Organizational security policies

In addition to those defined in the FPP base, the following organizational security policies are addressed by PP-compliant TOEs.

ID	Description
P.HIDE_NAT	The TOE shall be able to hide the IPv4 addresses of the entire IPv4 address space of the internal network.

3.5 Assumptions

No assumptions in addition to those defined in the FPP base are to be covered for the TOE.

4. Security objectives

4.1 Security objectives for the TOE

The list of security objectives for the TOE is defined in the FPP. This EP does not extend that definition.

In addition to those security objectives defined in the FPP base, the following additional security objectives are applicable to PP-compliant TOEs.

ID	Description
O.HIDE_NAT	The TOE shall be able to hide the IPv4 addresses of the entire IPv4 address space of the internal network.

4.2 Security objectives for the environment

There are no security objectives for the environment in addition to those defined in the FPP.

4.3 Rationales

The following tables map security objectives to the environment defined by the threats, policies and assumptions, illustrating that each security objective

covers at least one threat, assumption or policy and that each threat, assumption or policy is covered by at least one security objective.

4.3.1 Security objectives coverage

The security objective coverage analysis provided in the FPP is extended with the following:

Objectives	SPD coverage
O.HIDE_NAT	P.HIDE_NAT

4.3.2 Security objective sufficiency

The security objective sufficiency analysis is provided in the FPP is extended with the following:

OSP	Rationale for the security objectives
P.HIDE_NAT	*The TOE shall be able to hide the IPv4 addresses of the entire IPv4 address space of the internal network.* This policy is addressed by: • The TOE shall be able to hide the IPv4 addresses of the entire IPv4 address space of the internal network. (O.HIDE_NAT)

5. Extended components definition

There are no extended components defined for this FPP extended package.

6. IT Security Requirements

Please consider the definition of the “Application note” and “ST author note” as defined in [FPP]. The operations on security requirements are following the conventions specified in chapter in the [FPP].

6.1 Security Function Policies

6.1.1 FIREWALL Information Flow Control SFP {NAT}

The TOE will implement an information flow control Security Function Policy (SFP) called “FIREWALL Information Flow Control SFP {NAT}” that is used for address translation and port transformation. The TSF shall enforce the SFP on the packets that are sent or received through the TOE from one external IT entity to another. The policy is named FIREWALL Information Flow Control SFP {NAT} to indicate that the information flow control SFP is implementing the NAT functionality.

The TSF shall enforce the FIREWALL Information Flow Control SFP {NAT} based on at least the following types of subject and information security attributes:

- Objects:
    - network packet of protocol IPv4, TCP, UDP or ICMP
- Security attributes:
    - presumed source IP address;
    - presumed destination IP address;
    - TOE interface on which the packet arrived;
    - TOE interface on which the packet is intended to leave, after a routing decision (if applicable);
    - service (protocol and port, if applicable);
    - protocol [assignment: protocol name]: NAT transaction ID.

The TSF shall permit an information flow if all of the following rules hold:

- The TSF shall translate the IPv4 addresses when traversing the firewall (NAT).
- The TSF shall translate IPv4 addresses of 1..n "internal" hosts of one network that are mapped onto one "public" IPv4 address of a different interface of the firewall (PAT).

6.2 Security Functional Requirements

6.2.1 FDP_IFC.2 {NAT} – Complete information flow control

FDP_IFC.2.1 {NAT} The TSF shall enforce the **FIREWALL Information Flow Control SFP {NAT}** on

a) subjects: packet filter;

b) information: packet of a supported protocol sent through the TOE from one external IT entity to another;

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 {NAT} The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

ST author note: The subject "packet filter" refers to the active entity inside the TOE that performs the NAT functionality. The ST author may want to refine this into the actual subsystem/module name of the specific TOE.

6.2.2 FDP_IFF.1 {NAT} – Simple security attributes

FDP_IFF.1.1 {NAT} The TSF shall enforce the **FIREWALL Information Flow Control SFP {NAT}** based on the following types of subject and information security attributes:

a) subject packet filter, with security attributes:

- **[selection: [assignment: *additional subject security attributes*], *none*]**

b) object network packet of a supported protocol, with security attributes:
- **presumed source IP address;**
- **presumed destination IP address;**
- **TOE interface on which the packet arrived;**
- **TOE interface on which the packet is intended to leave, after a routing decision (if applicable);**
- **service (protocol and port, if applicable);**
- **protocol [assignment: *protocol name*]: NAT transaction ID;**
- **[assignment: *additional information security attributes*].**

FDP_IFF.1.2 {NAT} The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
- **[selection: [assignment: *other default rules enforced by the TOE], no other rules*].**

FDP_IFF.1.3 {NAT} The TSF shall enforce the **following additional information flow control rules:**
- **Static IP address translation will translate the source and/or destination IP address to another IP address as defined in the rule.**
- **[assignment: *additional information flow control rules*].**

FDP_IFF.1.4 {NAT} The TSF shall explicitly authorise an information flow based on the following rules: **no explicit authorisation rules**.

FDP_IFF.1.5 {NAT} The TSF shall explicitly deny an information flow based on the following rules: **no explicit denial rules**.

Application Note: According to FDP_IFF.1.2 {NAT}, the actual NAT mechanism is defined in the respective NAT rule. If a TOE provides only one specific mechanism, then this detail of the rule is implicitly given by the TOE implementation.

ST author note: The ST author is not required, but may want to specify the available NAT mechanisms (e.g., by referencing to a standard) in FDP_IFF.1.2 {NAT} using a refinement operation or an application note.

ST author note: The item "protocol (…): NAT transaction ID" is to be repeated for each additional (2nd etc.) protocol that is supported by the SPF.

ST author note: NAT filtering has to be implemented in sequence with the implementation of the FIREWALL Information Flow Control SFP of the base FPP. This is to ensure that the Information Flow Control SFP of the base FPP cannot be circumvented by the NAT Extended Package. This also means that the ST author is allowed to extend the SFR for the FIREWALL Information Flow Control SFP of the base FPP and still be able to claim compliance with this extended package.

ST author note: The mapping of a NAT translation between the external and internal side of the firewall may be dependent on the protocol. The term "NAT transaction ID" is used as a placeholder for such information. The ST author is not required, but may want to specify in the ST (using a refinement operation or application note) how the flow handle is identified for a specific protocol and TOE.

6.2.1 FMT_MSA.3 {NAT} – Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **FIREWALL Information Flow Control SFP {NAT}** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow **nobody** to specify alternative initial values to override the default values when an object or information is created.

6.3 Security functional requirements rationale

This section provides the rationale for the internal consistency and completeness of the security functional requirements defined in this extended package.

6.3.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective and that each security objective is addressed by at least one SFR.

The table shall be interpreted as an extension of the base FPP coverage analysis.

	FDP_IFC.2 {NAT}	FDP_IFF.1 {NAT}	FMT_MSA.3 {NAT}
O.HIDE_NAT	X	X	
O.INITIAL			X

6.3.2 Sufficiency

The sufficiency analysis is provided in the base FPP. This EP does not extend that analysis.

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Objective	Security functions
O.HIDE_NAT	*The TOE shall be able to hide the IPv4 addresses of the entire IPv4 address space of the internal network.* This objective is addressed as part of the information flow control by the TOE since the TOE is mediating the

	information flow between the internal and external network. The information flow control and address translation is satisfied by the information flow SFRs in combination, FDP_IFC.2 {NAT} and FDP_IFF.1 {NAT} requiring that the policy is applied to all traffic between the internal and external interfaces.
O.INITIAL	*(This objective is stated in [FPP])* *Upon initial start-up of the TOE or during configuration, the TOE shall provide well-defined initial settings for security relevant functions.* This objective is achieved by requiring that static attributes provides restrictive default values. The NAT functionality uses restrictive default settings which cannot be modified (FMT_MSA.3 {NAT}).

6.4 Dependencies between security functional requirements

SFR	Dependencies	Note
FDP_IFC.2 {NAT}	FDP_IFF.1	Resolved by FDP_IFF.1 {NAT}
FDP_IFF.1 {NAT}	FDP_IFC.1	Resolved by FDP_IFC.2 {NAT}
	FMT_MSA.3	Resolved by FMT_MSA.3 {NAT}
FMT_MSA.3 {NAT}	FMT_MSA.1	Not resolved. The default values cannot be modified.
	FMT_SMR.1	Not resolved. The default values cannot be modified.

6.5 Security Assurance Requirements

The security assurance requirements and rationale are provided in the base FPP.