Applicability Issues of IPsec in NAT-PT
draft-lee-ipsec-nat-pt-applicability-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on May 7, 2009.

Abstract

NAT-PT (Network Address Translation - Protocol Translation) mechanism that has been deprecated in [RFC4966] comes into spotlight again. The use-cases that NAT-PT addresses still need to be discussed and the requirements persist in IPv6 transition work. This document discusses the applicability issues when applying IPsec protocol to NAT-PT mechanism.
Table of Contents

1. Introduction .................................................. 3
2. Terminology ................................................... 3
3. IPsec Support Scenarios in NAT-PT ............................ 3
   3.1. Case 1: Transport Mode Operation ...................... 4
   3.2. Case 2: Tunneling Mode Operation ..................... 4
4. IPsec Applicability Issues in NAT-PT ........................ 4
   4.1. Issues for Negotiation of NAT-Traversal in the IKE ..... 5
      4.1.1. Basic IP Operation Issue ......................... 5
      4.1.2. IDii Payload Type Issue .......................... 6
      4.1.3. IKE Phase 2 Step (Quick Mode) ................... 6
   4.2. Transport Mode Issues ..................................... 6
   4.3. Tunneling Mode Issues .................................... 7
5. IANA Considerations ........................................... 8
6. Security Considerations ....................................... 8
7. References ....................................................... 8
   7.1. Normative References ................................... 8
   7.2. Informative References .................................. 9
Authors’ Addresses .............................................. 9
Intellectual Property and Copyright Statements ................. 10
1. Introduction

NAT-PT (Network Address Translation - Protocol Translation) addresses the IPv6 deployment scenario where IPv6 only node in IPv6 only network communicates with IPv4 only node in IPv4 only network and vice versa.

However, the original NAT-PT [RFC2766] has a limitation on supporting IPsec applications. There exists a similar problem in the NAT. In order to solve the problem, a few solutions were proposed for IPsec NAT traversal [RFC3947][RFC3948].

This document discusses the applicability issues when applying IPsec protocol to NAT-PT mechanism.

2. Terminology

- IPv6-only node : A node that implements IPv6 and does not support IPv4 stack.
- IPv4-only node : A node that implements IPv4 and does not support IPv6 stack.
- NAT-PT : The NAT-PT refers to IPv4/IPv6 transition mechanism that translates an IPv4 address into an IPv6 address and vice versa [RFC2766].

3. IPsec Support Scenarios in NAT-PT

IPv6-only node can communicate with IPv4-only node via NAT-PT. To secure bi-directional traffic security between IPv6-only node and IPv4-only node in the NAT-PT environment, the IPv6-only node can use IPsec protocols[AH],[ESP] with two types of IPsec mode.

IPsec uses two protocols in order to provide traffic security -- Authentication Header(AH) and Encapsulation Security Payload (ESP). Both protocols are described in more detail in their respective RFCs [RFC2402][RFC2406].

These protocols may be applied alone or in combination with each other so as to provide a desired set of security services in IPv4 and IPv6.

In this document, we consider ESP protocol only in order to simplify scenarios. Each protocol supports two types of secure mode that can be applicable to NAT-PT: Transport mode and Tunnel mode. The detailed description of the two modes are discussed in the following section.
3.1. Case 1: Transport Mode Operation

Transport Mode is most commonly used to provide end-to-end security between IPv6-only and IPv4-only node across the NAT-PT. IPv6-only node initiates IKE negotiation with the IPv4-only node to make security association across the NAT-PT before encapsulating UDP Tunneling packet for NAT-PT traversal.

IPv6-only node ------------ NAT-PT----------------- IPv4-only node

| | Security Association 1--------------- |
| (ESP transport) |
| Security Association 2--------------- |
| (AH transport) |

Figure 1: Transport Mode in NAT-PT

3.2. Case 2: Tunneling Mode Operation

When Tunneling Mode is applied, the peer node is not involved in the IPsec steps. On the contrary to above scenario, IPv6-only and IPv4-only node are not the endpoints which negotiates security association. GW-1(Gateway), GW-2(Gateway) will be charge of the IKE negotiation and Tunneling for encapsulation/decapsulation procedures.

IPv6-only node ----GW-1-------- NAT-PT----------GW-2----- IPv4-only node

|--Security Association 1--  |
| (ESP transport) |
| Security Association 2----|
| (AH transport) |

Figure 2: Tunneling Mode in NAT-PT

4. IPsec Applicability Issues in NAT-PT

This section is split into two parts. The first part describes the issues related to applying the IKE Phase1, Phase2 of NAT-Traversal mechanism to NAT-PT environment.

The second part describes the detailed issues when applied with
Tunneling Mode and Transport Mode.

4.1. Issues for Negotiation of NAT-Traversals in the IKE

If there is no SA(Security Association) in IPv6-only node, it starts the IKE negotiation and creates the SAs when it finished negotiation. For example, IPv6 node implemented with Linux launches the Racoon that is the IKE Daemon to exchange IKE messages.

To support the IKE negotiation in NAT-PT, IPv6-only node sends the detection packets to the IPv4-only node in order to check the existence of NATs between the peers using a NAT-Traversal mechanism [RFC3947].

The following example is IKE Phase1 Exchange using NAT-Traversal with Main Mode (Authentication with pre-shared key) in NAT-PT:

IPv6 Node A          NAT-PT                      IPv4 Node B
-------------------------------
UDP(500,500) HDR, SA, VID --><---- UDP(500,X) HDR, SA, VID

UDP(500,500) HDR, KE, Ni, NAT-D, NAT-D --><---- UDP(500,X) HDR, KE, Ni, NAT-D, NAT-D

UDP(4500,4500) <non-ESP market> HDR*, IDii, HASH_I --><--- UDP(4500,Y)<non-ESP market>HDR*, IDir, HASH_R

--- Figure 3: NAT-Traversal in NAT-PT ---

ping6 aaaa:bbbb:cccc::129.254.114.20 -->

* NAT-PT Prefix : aaaa:bbbb:cccc::/96
* NAT-PT address pool :129.254.144.1-15
* Router Advertisement Prefix : 220:220:101a:3::1/64
* Node B : 129.254.114.20

4.1.1. Basic IP Operation Issue

IPv6 Node A wants to communicate with the IPv4 Node B in the NAT-PT. Thus, IPv6 Node A creates a packet with:
Internet-Draft   Applicability Issues of IPsec in NAT-PT   November 2008

Source Address, SA = 220:220:101a:3::213:d4ff:fec2:a2bd/64
(The /64 prefix is NAT-PT’s advertisement message)
Destination Address, DA = aaaa:bbbb:cccc::129.254.114.20/96
(NAT-PT PREFIX::/96)

This packet is routed to the NAT-PT gateway, where the packet will be
translated to IPv4 format [RFC2766].

i.e : SA = 129.254.114.1 (one of the NAT-PT’s IPv4 address pool),
DA = 129.254.114.20

4.1.2. IDii Payload Type Issue

This issue is caused by applying IKE to the NAT-PT environment
because IKE address identifier is being used as an identifier in IKE
Phase1 or Phase2 :

- IPv6 Node A sets the ID type value to ID_IPV6_ADDR(5) in the IDii
  payload
- IPv4 Node B receives the packet with IPv4 SRC, IPv4 DST whose
  addresses were changed in NAT-PT, but IDii payload’s Identifier
type still has a IPv6 address type.

Since the modification of IP source or destination address is
occurred in the NAT-PT, the IKE’s identifier will not match. Thus in
order to apply IPsec to NAT-PT, ID_FQDN or ID_USER_FQDN[RFC2766]
should be used in the identifier of peer node.

4.1.3. IKE Phase 2 Step(Quick Mode)

After the Phase1 step, the Phase2 of IKE operation starts to get
IPsec parameters such as the type of UDP encapsulated IPsec packets
in IKE’s Quick Mode.

These encapsulation modes are:

- UDP-Encapsulated-Tunnel          3
- UDP-Encapsulated-Transport       4

The two types of encapsulation mode can be support in NAT-PT, but due
to the issues in Section 4.2, it is recommended to use the transport
mode only in NAT-PT environment.

4.2. Transport Mode Issues

In case of applying the UDP-Encapsulated-Transport mode between IPv6
node and IPv4 node, both peers know how to calculate the incremental
TCP checksum. To solve the problem, [RFC3977] suggests the NAT-OA (NAT Original Address) payload. NAT-OA payload is included in the first and second packets of Quick Mode.

In the NAT-PT environment, Node A sends the NAT-OA Payload encapsulated UDP with IDii type is ID_IPv6_ADDR and IPv6 address embedded the Identifier data field.

If the IPv6 packet crosses the NAT-PT, the NAT-PT changes the outer header of the IPv6 packet into IPv4 header. But the NAT-OA in the payload is not changed, because the above transport layer is encrypted by authentication algorithm.

On receiving the packets to the IPv4 node, the packets may recalculate using NAT-OA payload to verify TCP/IP checksum. But, IPv4 node has only native IPv4 network protocol stack, so it cannot parse the NAT-OA option. This will may raise the issues for IPsec to apply in NAT-PT environment.

### 4.3. Tunneling Mode Issues

When a tunneling mode is applied to secure packets between peers, the outer IP header is changed by NAT-PT from IPv6 HDR to IPv4 HDR. This will cause the tunneling issue for IPsec application to the NAT-PT.

Below is a diagram for the tunneling mode:

**STEP-1 : /* Before Applying ESP/UDP from IPv6 Node */**

(IPv6 HDR)[TCP][DATA]

**STEP-2 : /* After Applying ESP/UDP from IPv6 Node */**

(IPv6 HDR)[UDP HDR][ESP HDR][IPv6 HDR][TCP][DATA][ESP Trailer][ESP AUTH]

**STEP-3 : /* via the NAT-PT */**

(IPv4 HDR)[UDP HDR][ESP HDR][IPv6 HDR][TCP][DATA][ESP Trailer][ESP AUTH]

The IPv4 Node is waiting the UDP-Encapsulated ESP packets on port 4500. The procedures for incoming packets below:

- On receiving the packets, IPv4 node removes outer IPv4 HDR and UDP HDR.
- Using a existing SA (Security Association) value, the packets will be decrypted by authentication algorithm using pre-shared key.

However, the decrypted IPv6 packet cannot forward to the local network protocol stack, because the IPv4 node did not support the
IPv6 header processing.

Therefore, the tunneling mode operation is not suitable for IPsec traversal for in the NAT-PT.

5. IANA Considerations

This draft does not require any actions from IANA.

6. Security Considerations

This document discusses IPsec applicability issues in NAT-PT and does not incur any additional security vulnerability.

7. References

7.1. Normative References


7.2. Informative References

[I-D.choi-v6ops-natpt-ipsec]
Choi, I., "IPsec support for NAT-PT in IPv6",
draft-choi-v6ops-natpt-ipsec-00 (work in progress),

Authors’ Addresses

Sangjin Jeong
ETRI
161 Gajeong-dong, Yuseong-gu
Daejeon, 305-700
Korea

Phone: +82-42-860-1877
Email: sjjeong@gmail.com

Myung-Ki Shin
ETRI
161 Gajeong-dong, Yuseong-gu
Daejeon, 305-700
Korea

Phone: +82-42-860-4847
Email: mkshin@etri.re.kr

Sangdo Lee
TmaxSoft
272-6 Seohyeon-dong, Bundang-gu
Sungnam,
Korea

Phone:
Email: doyaa2@gmail.com
Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.