

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 15, 2008

H. Deng
China Mobile
Y. Ma
Hitachi
Y. Wu
ZTE USA
June 13, 2008

**GRE key as the traffic selector for IPsec tunnel
draft-deng-ipsec-gre-key-ts-00**

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 December 15, 2008.

Abstract

This document describes the IPsec Tunnel based on GRE key as the traffic selector. When GRE key is used in IP packet transmission scenario of the wireless communication. Several enterprise need different security policy when transmit the packet through some unguaranteed Internet cloudy. This document propose to adopt GRE key as the IPsec traffic selector.

Table of Contents

1.	Introduction	3
2.	Network Scenario	4
3.	GRE key as IPsec traffic selector	6
4.	Security Considerations	7
5.	IANA Consideration	8
6.	Conclusion	9
7.	Normative References	10
	Authors' Addresses	11
	Intellectual Property and Copyright Statements	12

1. Introduction

GRE key has been used to allocate to encapsulate the traffic between two IP access gateways in many ways including the 3GPP [[TS23.402](#)].

Some company have some branch office would like to access from wireless Internet communication technologies, and coincidently some operator's mobile Internet is mixed together with public Internet, in such scenario, they may need different security policy for each connections.

In such scenarios, GRE key as the IPsec traffic selector is proposed.

2. Network Scenario

In some wireless communication, some IP mobility management protocol has mandate the IPsec tunnel between different mobility agents.

Private addressing is common for user address allocation by operators. As shown in Fig. 1, if users from different enterprise headquarter (A and B) roaming to the same visited network and the same private address is allocated to users, the access router need to differentiate data from the users. In this case GRE key will be used to identify the tunnel from different users.

IPsec can be used to protect the GRE encapsulated packets. Operator can have its own security policy on whether to secure the data for users of different operators. For example, if user is from enterprise A, the data will be protected by some security policy. If the user is from enterprise B, the data will be protected differently.

In such case, it is impossible to differentiate packets from different users by using current traffic selector defined in IPsec. GRE key is necessary to be a traffic selector for Operator to deploy the security policy.

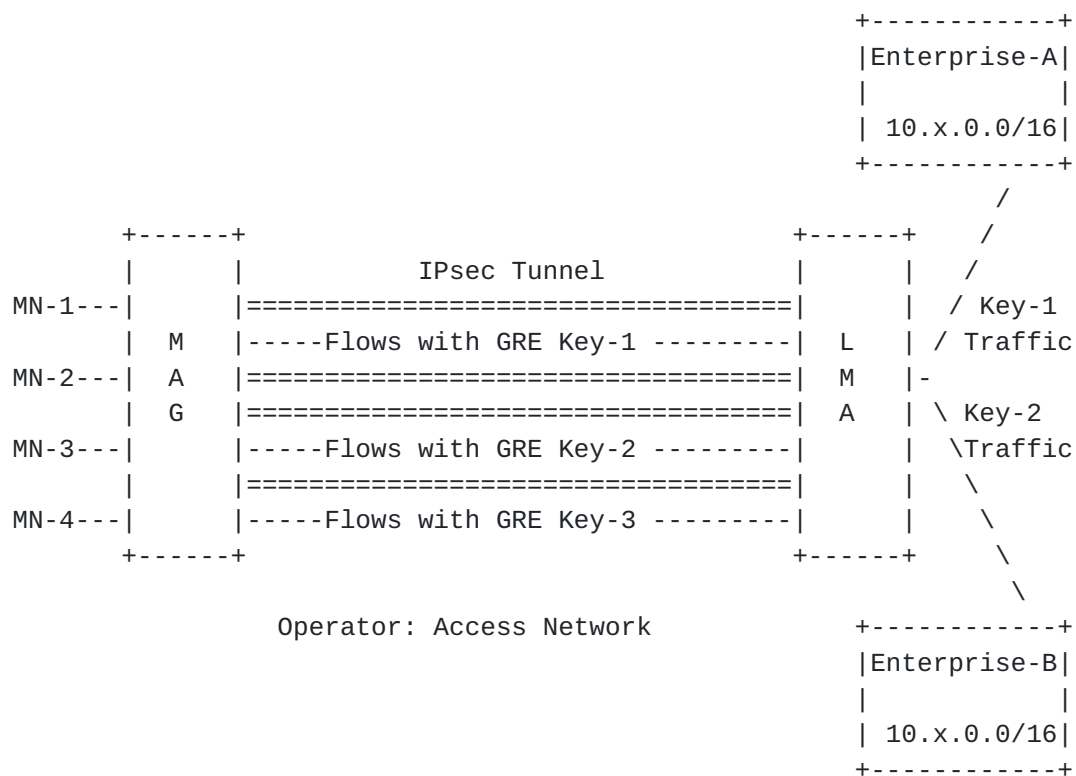


Figure 1: Network scenario for GRE key based IPsec Tunnel

3. GRE key as IPsec traffic selector

Current IKE/IPsec implementation does not support GRE key as the traffic selector. Extensions for IKE/IPsec is needed to support GRE key.

4. Security Considerations

IPsec tunnel has been used for protecting data transmission between two mobility agents.

5. IANA Consideration

This document defines no encodings, hence there are no IANA considerations.

6. Conclusion

This document describes a GRE key as traffic selector based IPsec tunnel mechanism.

7. Normative References

- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), December 2005.
- [TS23.402] 3GPP, "TS 23.402: Architecture enhancements for non-3GPP accesses", March 2008,
<<http://www.3gpp.org/ftp/Specs/html-info/23402.htm>>.

Authors' Addresses

Hui Deng
China Mobile
53A,Xibianmennei Ave.,
Xuanwu District,
Beijing 100053
China

Email: denghui02@gmail.com

Yuanchen Ma
Hitachi
2, Kexueyuan Nanlu
Haidian District,
Beijing 100053
China

Email: ycma610103@gmail.com

Yingzhe Wu
ZTE USA
10105 Pacific Heights Blvd, Suite 250
San Diego, CA 92121
USA

Email: yingzhe.wu@zteusa.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.

