

Internet Draft
Category: Standards Track
Expiration Date: August 25, 2008

Lou Berger (LabN)
Russ White (Cisco Systems)
Eric Rosen (Cisco Systems)

February 25, 2008

BGP IPsec Tunnel Encapsulation Attribute

[draft-berger-idr-encaps-ipsec-01.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/lid-abstracts.html>

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

This Internet-Draft will expire on August 25, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

The BGP Encapsulation Subsequence Address Family Identifiers (SAFI) provides a method for the dynamic exchange of encapsulation information, and the indication of encapsulation protocol types to be used for different next hops. Currently support for GRE and L2TPv3 tunnel types are defined. This document defines support for IPsec tunnel types.

Internet-Draft [draft-berger-idr-encaps-ipsec-01.txt](#) February 25, 2008

Contents

1	Introduction	3
1.1	Conventions used in this document	3
2	IPsec Tunnel Encapsulation Types	3
3	Use of IPsec	4
4	IPsec Tunnel Authenticator sub-TLV	4
4.1	Use of the IPsec Tunnel Authenticator sub-TLV	5
5	Security Considerations	5
6	IANA Considerations	6
7	References	6
7.1	Normative References	6
7.2	Informative References	7
8	Acknowledgments	8
9	Authors' Addresses	8
10	Full Copyright Statement	8
11	Intellectual Property	9

Internet-Draft [draft-berger-idr-encaps-ipsec-01.txt](#) February 25, 2008

[1.](#) Introduction

The BGP [[RFC4271](#)] Encapsulation Subsequence Address Family Identifiers (SAFI) allows for the communication of tunnel information and the association of this information to a BGP next hop. The Encapsulation SAFI can be used to support the mapping of prefixes to next hops and tunnels of the same address family, IPv6 prefixes to IPv4 next hops and tunnels using [[RFC4798](#)], and IPv4 prefixes to IPv6 next hops and tunnels using [[V4NLRI-V6NH](#)]. The Encapsulation SAFI can also be used to support the mapping of VPN prefixes to tunnels when VPN prefixes are advertised per [[RFC4364](#)] or [[RFC4659](#)]. [[SOFTWIRES](#)] provides useful context for the use of the Encapsulation SAFI.

The Encapsulation SAFI is defined in [[ENCAPS-SAFI](#)]. [[ENCAPS-SAFI](#)] also defines support for the GRE [[RFC2784](#)] and L2TPv3 [[RFC3931](#)] tunnel types. This document builds on [[ENCAPS-SAFI](#)] and defines support for IPsec tunnels. Support is defined for IP Authentication Header in Tunnel-mode (AH), [[RFC4302](#)], and for IP Encapsulating Security Payload in Tunnel-mode (ESP), [[RFC4303](#)]. Support for IP-in-IP, [[RFC2003](#)], and MPLS-in-IP, [[RFC4023](#)] protected by IPsec Transport Mode is also defined.

The Encapsulation NLRI Format is not modified by this document.

[1.1.](#) Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

[2.](#) IPsec Tunnel Encapsulation Types

Per [[ENCAPS-SAFI](#)], tunnel type is indicated in the Tunnel Encapsulation attribute. This document defines the following tunnel type values:

- AH in Tunnel-mode: Tunnel Type = 3
- ESP in Tunnel-mode: Tunnel Type = 4
- IP-in-IP Tunnel with IPsec Transport Mode: Tunnel Type = 5

Internet-Draft [draft-berger-idr-encaps-ipsec-01.txt](https://datatracker.ietf.org/doc/draft-berger-idr-encaps-ipsec-01.txt) February 25, 2008

- MPLS-in-IP Tunnel with IPsec Transport Mode: Tunnel Type = 6

Note, see Section 4.3 of [[ENCAPS-SAFI](#)] for a discussion on the advertisement and use of multiple tunnel types.

This document does not specify the use of the sub-TLV types defined in [[ENCAPS-SAFI](#)] with these tunnel types. See below for the definition of an IPsec tunnel type specific sub-TLV.

[3.](#) Use of IPsec

If a R1 is a BGP speaker that receives an Encapsulation SAFI update from another BGP speaker, R2, then if R1 has any data packets for which R2 is the BGP next hop, R1 MUST initiate an IPsec SA of the specified "tunnel type", and all such data packets MUST be sent through that SA.

Let R1 and R2 be two BGP speakers that may send data packets through R3, such that the data packets from R1 and from R2 may be received by R3 over the same interface. Then if R3 has sent an update containing an Encapsulation SAFI, and if this update specifies an IPsec tunnel type, and if this update is received by R2, and an Encapsulation-SAFI with an IPsec tunnel type, MUST also be received by R1. That is, on a given interface, if IPsec is required for any data packets, it MUST be required for all. It does not necessarily need to be required for control packets that are directly addressed to R3.

Security policy has the granularity of BGP speaker to BGP speaker. The required security policies must be configured into the BGP speakers, and the policy for each SA is negotiated via IKE.

[4.](#) IPsec Tunnel Authenticator sub-TLV

This document defines a new sub-TLV for use with the Tunnel Encapsulation Attribute defined in [[ENCAPS-SAFI](#)]. The new sub-TLV is referred to as the "IPsec Tunnel Authenticator sub-TLV" and MAY be included in any Encapsulation SAFI NLRI ([[ENCAPS-SAFI](#)]) indicating a Tunnel Type defined in this document. Support for the IPsec Tunnel Authenticator sub-TLV MUST be implemented whenever the tunnel types defined in this document are implemented. However, its use is OPTIONAL, and is a matter of policy.

The sub-TLV type of the IPsec Tunnel Authenticator sub-TLV is 3. The sub-TLV length is variable. The structure of the sub-TLV is as follows:

- Authenticator Type: two octets

This document defines authenticator type 1, "SHA-1 hash of public key", as defined in [section 3.7 of RFC 4306](#).

- Value: (variable)

A value used to authenticate the BGP speaker that generated this NLRI. The length of this field is is not encoded explicitly, but can be calculated as (sub-TLV length - 2).

In the case of authenticator type 1, this field contains the 20-octet value of the hash.

A BGP speaker which sends the IPsec Tunnel Authenticator sub-TLV with authenticator type 1 MUST be configured with a certificate containing the public key whose hash is sent in the value field of the sub-TLV. This certificate MAY be self-signed.

[4.1.](#) Use of the IPsec Tunnel Authenticator sub-TLV

If a IPsec Tunnel Authenticator sub-TLV with authenticator type 1 is present in the Encapsulation SAFI update, then R1 (as defined above in [Section 3](#)) must use IKE to obtain a certificate from R2 (as defined above in [Section 3](#)), and R2 must send a certificate containing the public key whose hash occurred in the value field of the IPsec Tunnel Authenticator sub-TLV. R1 MUST NOT attempt to establish an SA to R2 UNLESS the public key in the certificate hashes to the same value that occurs in the IPsec Tunnel Authenticator sub-TLV.

[5.](#) Security Considerations

This document uses IP based tunnel technologies to support data plane transport. Consequently, the security considerations of those tunnel technologies apply. This document defines support for IPsec AH [[RFC4302](#)] and ESP [[RFC4303](#)]. The security considerations from those documents apply to the data plane aspects of this document.

As with [[ENCAPS-SAFI](#)], any modification of the information that is used to form encapsulation headers, or to choose a tunnel type, or to choose a particular tunnel for a particular payload type, user data

packets may end up getting misrouted, misdelivered, and/or dropped. Misdelivery is less of an issue when IPsec is used as such misdeldelivery is likely to result in a failure of authentication or decryption at the receiver. Furthermore, in environments where authentication of BGP speakers is desired, the IPsec Tunnel Authenticator sub-TLV defined in [Section 4](#) may be used.

More broadly, the security considerations for the transport of IP reachability information using BGP are discussed in [[RFC4271](#)] and [[RFC4272](#)], and are equally applicable for the extensions described in this document.

[6.](#) IANA Considerations

IANA is requested to administer assignment of new namespaces and new values for namespaces defined in this document and reviewed in this section.

Upon approval of this document, the IANA will make the assignment in the Tunnel TLVs and sub-TLVs section of the registry.

Tunnel Type	Reference
-----	-----
AH:	Type = 3 [This document]
ESP:	Type = 4 [This document]
IP-in-IP tunnel	
with IPsec Transport Mode:	Type = 5 [This document]
MPLS-in-IP tunnel	
with IPsec Transport Mode:	Type = 6 [This document]

Tunnel Type	Sub-TLV Type	Reference
-----	-----	-----
3,4,5,6	IPsec Tunnel Authenticator:	Type = 3 [This document]

[7.](#) References

[7.1.](#) Normative References

- [ENCAPS-SAFI] Mohapatra, P., Rosen, E., "BGP Information SAFI and BGP Tunnel Encapsulation Attribute", Work in Progress, [draft-ietf-idr-encaps-safi-00.txt](#), August 2007.

- [RFC4271] Rekhter, Y., Ed. et al, "A Border Gateway Protocol 4 (BGP-4)", [RFC 4271](#), January 2006.

[7.2.](#) Informative References

- [RFC2003] Perkins, C., "IP Encapsulation within IP", [RFC 2003](#), October 1996.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," [RFC 2119](#).

- [RFC2784] Farinacci, D., et al, "Generic Routing Encapsulation (GRE)", [RFC 2784](#), March 2000.
- [RFC3931] Lau, J., Ed., et al, "Layer Two Tunneling Protocol - Version 3 (L2TPv3)", [RFC 3931](#), March 2005.
- [RFC4023] Worster, T., Rekhter, Y., Rosen, E., Ed., "Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)", [RFC 4023](#), March 2005.
- [RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", [RFC 4272](#), January 2006.
- [RFC4302] Kent, S., "IP Authentication Header", [RFC 4302](#), December 2005.
- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)" [RFC 4303](#), December 2005.
- [RFC4364] Rosen, E., Rekhter, Y., "BGP/MPLS IP Virtual Private Networks (VPNs)", [RFC 4364](#), February 2006.
- [RFC4659] De Clercq, J., et al, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN", [RFC 4659](#), September 2006.
- [RFC4798] J. De Clercq, D. Ooms, S. Prevost, F. Le Faucheur, "Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge Routers (6PE)", [RFC 4798](#), February 2007.
- [SOFTWIRES] Wu, J. et al, "Softwire Mesh Framework", Work in Progress, [draft-ietf-softwire-mesh-framework-03.txt](#), January 2008.

- [V4NLRI-V6NH] F. Le Faucheur, E. Rosen, "Advertising an IPv4 NLRI with an IPv6 Next Hop", Work in Progress, [draft-ietf-idr-v4nlri-v6nh-01.txt](#), October 2007.

8. Acknowledgments

The authors wish to thank Sam Hartman and Tero Kivinen for their help with the security-related issues. However, it should be noted that they have not reviewed this revision of the draft.

9. Authors' Addresses

Lou Berger
LabN Consulting, L.L.C.
Phone: +1-301-468-9228
Email: lberger@labn.net

Russ White
Cisco Systems
Email: riw@cisco.com

Eric C. Rosen
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA, 01719
Email: erosen@cisco.com

10. 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.

11. 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.

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

Generated on: Thu Feb 21 12:11:30 EST 2008