Network Working Group
Request for Comments: 5566
Category: Standards Track

L. Berger
LabN
R. White
E. Rosen
Cisco Systems

June 2009

BGP IPsec Tunnel Encapsulation Attribute

Status of This Memo

Copyright Notice

Abstract

The BGP Encapsulation Subsequent Address Family Identifier (SAFI) provides a method for the dynamic exchange of encapsulation information and for the indication of encapsulation protocol types to be used for different next hops. Currently, support for Generic Routing Encapsulation (GRE), Layer 2 Tunneling Protocol (L2TPv3), and IP in IP tunnel types are defined. This document defines support for IPsec tunnel types.

Table of Contents

1. Introduction

The BGP [RFC4271] Encapsulation Subsequent Address Family Identifier (SAFI) allows for the communication of tunnel information and for 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 [RFC5549]. 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]. [RFC5565] provides useful context for the use of the Encapsulation SAFI.

The Encapsulation SAFI is defined in [RFC5512]. [RFC5512] also defines support for the GRE [RFC2784], L2TPv3 [RFC3931], and IP in IP [RFC2003] tunnel types. This document builds on [RFC5512] and defines support for IPsec tunnels. Support is defined for IP Authentication Header (AH) in tunnel mode [RFC4302] and for IP Encapsulating Security Payload (ESP) in tunnel mode [RFC4303]. The IPsec architecture is defined in [RFC4301]. Support for IP in IP [RFC2003] and MPLS-in-IP [RFC4023] protected by IPsec Transport Mode is also defined.

The Encapsulation Network Layer Reachability Information (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. Tunnel Encapsulation Types

Per [RFC5512], tunnel type is indicated in the Tunnel Encapsulation attribute. This document defines the following tunnel type values:

- Transmit tunnel endpoint: Tunnel Type = 3

- IPsec in Tunnel-mode: Tunnel Type = 4 [RFC4302], [RFC4303]

- IP in IP Tunnel with IPsec Transport Mode: Tunnel Type = 5 [RFC2003], [RFC4303]

- MPLS-in-IP Tunnel with IPsec Transport Mode: Tunnel Type = 6 [RFC4023]

  Note, see Section 4.3 of [RFC5512] for a discussion on the advertisement and use of multiple tunnel types.

  Note, the specification in [RFC4023] for MPLS-in-IP tunnels with IPsec Transport mode applies as well to IP in IP tunnels.

This document does not specify the use of the sub-TLV types defined in [RFC5512] with these tunnel types. See below for the definition of a specific sub-TLV for use with the defined tunnel types.

3. Use of IPsec Tunnel Types

The IPsec tunnel types are defined above with the values 4, 5, and 6. If 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 (security association) 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. In this case, when R3 sends an Encapsulation SAFI that indicates an IPsec tunnel type to R2, then R3 SHOULD also send an update specifying an Encapsulation SAFI with an IPsec tunnel type to R1. That is, on a given interface, if IPsec is required for any data packets, it SHOULD be required for all. This eliminates dependence on the IPsec selector mechanisms to correctly distinguish traffic that needs to be protected from traffic that does not.

Security policy has the granularity of BGP speaker to BGP speaker. The required security policies must be configured into the BGP speakers. Policies for each SA will typically be established using

IKEv2 (Internet Key Exchange) [RFC4306], with either public-key or pre-shared key authentication. The SA MAY also be configured via manual techniques. Manual configuration specification and considerations are defined in [RFC4301], [RFC4302], and [RFC4303] (and includes keys, Security Parameter Index (SPI) numbers, IPsec protocol, integrity/encryption algorithms, and sequence number mode).

4. IPsec Tunnel Authenticator sub-TLV

This document defines a new sub-TLV for use with the Tunnel Encapsulation attribute defined in [RFC5512]. The new sub-TLV is referred to as the "IPsec Tunnel Authenticator sub-TLV", and one or more of the sub-TLVs MAY be included in any Encapsulation SAFI NLRI [RFC5512] 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 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 that sends the IPsec Tunnel Authenticator sub-TLV with authenticator type 1 MUST be configured with a private key / public key pair, the public key being the key whose hash is sent in the value field of the sub-TLV. The BGP speaker MUST either (a) be able to generate a self-signed certificate for the public key, or else (b) be configured with a certificate for the public key.

When the IPsec Tunnel Authenticator sub-TLV is used, it is highly RECOMMENDED that the integrity of the BGP session itself be protected. This is usually done by using the TCP MD5 option [RFC2385].

4.1. Use of the IPsec Tunnel Authenticator sub-TLV

If an 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 IKEv2 [RFC4306] to obtain a certificate from R2 (as defined above in Section 3), and R2 MUST send a certificate for 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 one of the IPsec Tunnel Authenticator sub-TLVs.

R2 MUST also perform the reciprocal processing. Specifically, when establishing an SA from R1 and R1 has advertised the IPsec Tunnel Authenticator sub-TLV with authenticator type 1, R2 MUST use IKEv2 [RFC4306] to obtain a certificate from R1, and R1 MUST send a certificate for the public key whose hash occurred in the value field of the IPsec Tunnel Authenticator sub-TLV. R2 MUST NOT attempt to establish an SA to R1 UNLESS the public key in the certificate hashes to the same value that occurs in one of the IPsec Tunnel Authenticator sub-TLVs.

Note that the "Transmit tunnel endpoint" tunnel type (value = 3) may be used by a BGP speaker that does not want to be the receiving endpoint of an IPsec tunnel but only the transmitting endpoint.

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 as well as [RFC4301] apply to the data plane aspects of this document.

As with [RFC5512], any modification of the information that is used to form encapsulation headers, to choose a tunnel type, or to choose a particular tunnel for a particular payload type may lead to user data packets getting misrouted, misdelivered, and/or dropped. Misdelivery is less of an issue when IPsec is used, as such misdelivery 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.

If the integrity of the BGP session is not itself protected, then an imposter could mount a denial-of-service attack by establishing numerous BGP sessions and forcing an IPsec SA to be created for each one. However, as such an imposter could wreak havoc on the entire routing system, this particular sort of attack is probably not of any special importance.

It should be noted that a BGP session may itself be transported over an IPsec tunnel. Such IPsec tunnels can provide additional security to a BGP session. The management of such IPsec tunnels is outside the scope of this document.

6. IANA Considerations

IANA administers the assignment of new namespaces and new values for namespaces defined in this document and reviewed in this section.

IANA has made the following assignments in the "BGP Tunnel Encapsulation Attribute Tunnel Types" registry.

Value	Name	Reference
3	Transmit tunnel endpoint	[RFC5566]
4	IPsec in Tunnel-mode	[RFC5566]
5	IP in IP tunnel with IPsec Transport Mode	[RFC5566]
6	MPLS-in-IP tunnel with IPsec Transport Mode	[RFC5566]

IANA has made the following assignment in the "BGP Tunnel Encapsulation Attribute Sub-TLVs" registry.

Value	Name	Reference
3	IPsec Tunnel Authenticator	[RFC5566]

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4306] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC5512] Mohapatra, P. and E. Rosen, "The BGP Encapsulation Subsequent Address Family Identifier (SAFI) and the BGP Tunnel Encapsulation Attribute", RFC 5512, April 2009.

7.2. Informative References

[RFC2003] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.

[RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

[RFC3931] Lau, J., Ed., Townsley, M., Ed., and I. Goyret, Ed., "Layer Two Tunneling Protocol - Version 3 (L2TPv3)", RFC 3931, March 2005.

[RFC4023] Worster, T., Rekhter, Y., and E. Rosen, 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.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.

[RFC4659] De Clercq, J., Ooms, D., Carugi, M., and F. Le Faucheur, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN", RFC 4659, September 2006.

[RFC4798] De Clercq, J., Ooms, D., Prevost, S., and F. Le Faucheur, "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)", RFC 4798, February 2007.

[RFC5549] Le Faucheur, F. and E. Rosen, "Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop", RFC 5549, May 2009.

[RFC5565] Wu, J., Cui, Y., Metz, C. and E. Rosen, "Softwire Mesh Framework", RFC 5565, June 2009.

8. Acknowledgments

The authors wish to thank Sam Hartman and Tero Kivinen for their help with the security-related issues.

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