Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 25, 2013

X. Zhang
Juniper Networks
T. Tsou
Futurewei Technologies
W. Liu
Huawei Technologies

October 22, 2012

Multiple Path IP Security
draft-zhang-ipsecme-multi-path-ipsec-02

Abstract

This document presents one approach to enhance data protection when transmitting IPsec datagrams across the insecure networks. The method affords the stronger protection to the traffic by splitting it among a set of sub-tunnels. All the Security Associations (SAs) are set up independently for all sub-tunnels. Both the sending and receiving entity combine all the sub-tunnels to one clustered tunnel. As different sub-tunnel uses different crypto key materials and processing parameters, it may achieve the stronger protection of the traffic across the insecure networks. In addition, it could possibly bring more benefits in terms of the network control.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on April 25, 2013.

Copyright Notice

Table of Contents

1. Introduction

IPsec protocols suite specifies the base architecture for IPsec-compliant systems. It describes how to provide a set of security services for traffic at the IP layer, in both the IPv4 and IPv6 environments. It defines security association (SA) as the fundamental concept to IPsec, which defines a simplex "connection" that affords security services to the traffic carried by it. Security services are afforded to an SA by the use of AH [RFC4302], or ESP [RFC4303], but not both. If both AH and ESP protection are applied to a traffic stream, then two SAs must be created and coordinated to effect protection through iterated application of the security protocols.

Since one SA is used to carry uni-cast traffic, a pair of SAs must be established in point-to-point communication. The two SAs create one uni-cast IPsec tunnel between two security gateways. In order to differentiate different SAs, the Security Parameters Index (SPI), one 32-bit value, is used by a receiver to identify the SA to which an incoming packet should be bound. The SPI assignment is done at the creator of the SA, or usually the receiving side. At the sending side, additional destination IP address information can be used to resolve the SPI conflict. In this way, the sending side can select the correct SA under which IP packet will be processed. In this document, the new method also makes use of multiple SPIs. Nevertheless, it enhances the security service in different way from SA.

2. Terminology

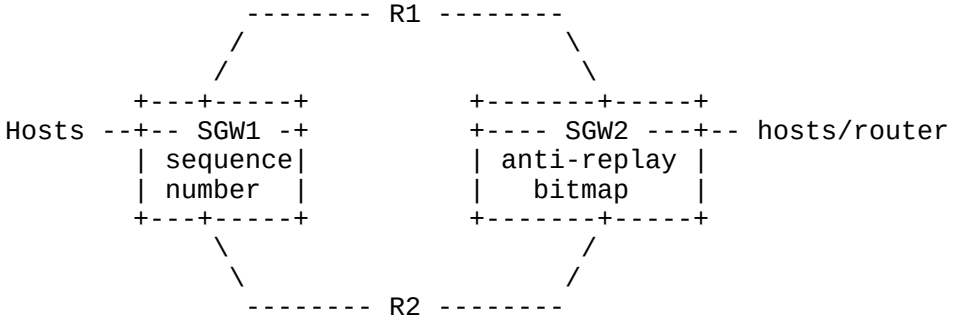
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Multiple Path IPsec

Data confidentiality is the protection of transmitted data from passive attacks, such as eavesdropping. In current IPsec implementation, all the IP datagrams transmitted inside one IPsec tunnel are afforded protection by one SA. In order to enhance the confidential security service, we use a set of SAs to protect the traffic. We propose to set up multiple tunnels between two entities and then cluster them together to form one clustered tunnel. One IP packet is still protected by one single SA. The sending entity just splits the traffic among all these SAs. The receiving entity must multiplex the traffic from the different IPsec tunnels. All these

tunnels clustered together are termed "sub-tunnels". The SAs for these sub-tunnels are termed "sub-SA". The IP traffic, which should be protected inside one clustered tunnel, is split among all the sub-tunnels. The term "security association cluster", or "SA cluster", is used to describe the combination of SAs through which the traffic must be processed to satisfy a security policy.

As multiple sub-tunnels are set up for the same flow of traffic between two secure entities, the physical paths may be different. The processing order of these clustered SAs is only local matter as all these SAs are not nested SAs.



3.1. The SA setup

The SA cluster setup consists of multiple sub-SA setups. All these sub-tunnels are set up independently. After setup, the sub-tunnel can be added to the cluster one by one. But it is the local matter as how to add the sub-SAs into the SA cluster. All the collaborative sub-tunnels have different SPI values. There is no limitation on how many sub-tunnels can be used for one clustered tunnel. Both the sending entity and receiving entity agree on SA cluster which will be used before any IPsec traffic goes through any of these sub-tunnels. After the traffic flows inside clustered tunnel, new SA can still be able to set up and join the SA cluster.

Even though all the sub-tunnels are independent, they share only one sequence number source. The IPsec packet carried inside the clustered tunnel has unique sequence number.

3.2. The outbound packet processing

The sending entity splits or alternates the IPsec traffic through different sub-tunnels. When the SA cluster is selected for the traffic processing based on security policy configuration, one sub-SA is chosen for outbound IPsec processing only for that packet. It is the local implementation that determines which SA should be applied

to the specific IP packet. Except that the sequence number is shared among all sub-SAs, all the other processing procedures are not altered. A local implementation at sending entity can choose any method to obtain the sequence number for this packet, which is independent of sub-SA.

3.3. The inbound packet processing

The selection of sub-SA is the same as the selection of single SA, which is based on SPI and IP address information. Except that the sequence number processing is a bit different, all other aspects are not changed.

With the use of multiple sub-tunnels, by its nature, it could cause out-of-order delivery of IPsec packets for the secure communication channel between two entities. As the remedy, the sequence number in IPsec header can be used if the receiving entity needs to maintain the sending order.

If anti-replay is enabled, all these sub-tunnels will use one shared anti-replay bitmap at the receiving entity. The anti-replay check is done against the SA cluster instead of sub-SA. But it does not change how anti-replay is done.

3.4. The SA expiration

If sub-SA is negotiated through IKE negotiation, it may have its own soft and hard lifetime. But there is no lifetime for SA cluster. There is no change as to maintenance of each sub-SA.

If one sub-SA becomes invalid, it could not be used for further packet processing. If SA cluster does not hold any valid sub-SA, it becomes invalid too.

3.5. Multiple paths

All these sub-tunnels are set up independently. The traffic through the different sub-tunnels can go the same route. It can also go the different routes based on the routing policy. The path selection algorithm is out the scope of this document.

3.6. Interoperability

In case that SA cluster contains only one sub-SA, it must not have any interoperability issue with the current IPsec implementation if the current one does not support SA cluster.

3.7. Reorder packets

The solution of multipath introduces the issue of the possibility of out of order delivery. Actually, this is the only solution which causes the disorder problem. Even with single SA, it can also bring in the out of order problem. Technically, the reorder process be can be done at aggregate node or end host, based on the topology of network, just like TCP reorder or IP reassembly [RFC5236][Zhang02]. The reorder algorithm is out the scope of this document.

4. The benefit for SA cluster

The method enhances the security service by spreading the traffic onto multiple paths. For example, it makes it harder for the attacker to intercept all the packets if different routes are used. Even with the same route used, it is harder for the attacker to know which set of SAs are clustered SA, thus harder to decrypt the intercepted packets. With multiple paths selected, it provides high reliability especially in case of link failure. It also provides the option for optimized performance and optimal network control, which is not covered in this document.

5. Acknowledgements

Wait for comments.

6. Security Considerations

This document intends to enhance the security service which IPsec provides. SA cluster provides the option to perform the different cryptographic transformation on the different packet. In addition, it also provides the option to transmit the packets along the different paths.

7. IANA Considerations

None.

8. References

8.1. Normative References

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

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

8.2. Informative References

[Piratla06] N. M. Piratla, et al., "Reordering of Packets due to Multipath Forwarding - An Analysis", 2006.

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

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

[RFC5236] Jayasumana, A., Piratla, N., Banka, T., Bare, A., and R. Whitner, "Improved Packet Reordering Metrics", RFC 5236, June 2008.

[Zhang02] M. Zhang, et al., "Improving TCP's Performance under Reordering with DSACK", 2002.

Authors' Addresses

Xiangyang Zhang
Juniper Networks
1194 N. Mathilda Ave
Sunnyvale, CA 94089
USA

Email: vzhang2008@yahoo.com

Tina Tsou
Futurewei Technologies
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4424
Email: tina.tsou.zouting@huawei.com

Will Liu
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: liushucheng@huawei.com