IPSECME WG
Internet Draft
Intended status: Informational
Expires: October 22, 2011

Jitender Arora
Prashant Kumar
Acme Packet
April 22, 2010

Alternate Tunnel Addresses for IKEv2
draft-arora-ipsecme-ikev2-alt-tunnel-addresses-00

Status of this Memo

Copyright and License Notice

Abstract

IKEv2 is a protocol for setting up Virtual Private Network (VPN) tunnels from a remote location to a gateway so that the VPN client can access services in the network behind the gateway. Currently the IKE SAs and tunnel mode Ipsec SA's are created implicitly between the IP addresses that are used when the IKE_SA is established. These IP addresses are then used as the outer (tunnel header) addresses for tunnel mode IPSEC packets (transport mode IPsec SAs are beyond the scope of this document). This document defines an IKEv2 extension that allows the outer tunnel header addresses for the tunnel mode IPSEC packets to be different than the IKE peer IP addresses.

Table of Contents

1. Introduction....2
2. Terminology....3
3. IKEv2 IKE_AUTH exchange with different Tunnel Address....3
4. IKEv2 CREATE_CHILD_SA exchange with different Tunnel Address4
5. Usage Scenarios....5
5.1. IKEv2 signaling and the IPSEC tunnel mode traffic on different addresses....5
6. NAT Scenarios and Routing issues....5
7. Alternate Tunnel address messages....6
7.1. DIFFERENT_TUNNEL_ADDRESS_SUPPORTED....6
7.2. TUNNEL_ADDRESS....6
8. IANA Considerations....7
9. Security Considerations....8
9.1. Different Tunnel Addresses and Hijacking....8
10. Acknowledgements....9
11. Informative References....9
11.1. Normative References....9
11.2. Informative References....9
Author's Address....10

1. Introduction

IKEv2 [2] is used for setting up IPsec [8] based VPNs. Currently the IKE SAs and tunnel mode Ipsec SA's are created implicitly between the IP addresses that are used when the IKE_SA is established. These IP addresses are then used as the outer (tunnel header) addresses for tunnel mode IPSEC packets. This imposes a limitation that all the Ikev2 signaling and the IPSEC traffic needs to go to the same address on the gateway. This document defines an IKEv2 extension that allows the outer tunnel header addresses for the tunnel mode IPSEC packets

to be different than the IKE peer IP addresses.

This document proposes an alternate Tunnel address mechanism for IKEv2 that enables a VPN gateway or the VPN client use the different tunnel address for the IPSEC packets than the one which is being used for the IKE negotiation. The tunnel address can be specified during the IKE_AUTH exchange and also during the CREATE_CHILD_SA exchange.

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 [1].

3. IKEv2 IKE_AUTH exchange with different Tunnel Address

This section describes the use of different Tunnel Address mechanism during the IKE_AUTH exchange. The use of different tunnel address during CREATE_CHILD_SA exchange are explained in subsequent sections.

The VPN client indicates support for the IKEv2 different tunnel address mechanism and the willingness to send or receive the traffic on tunnel addresses different than the IKE peer addresses by including a DIFFERENT_TUNNEL_ADDRESS_SUPPORTED notification message in the initial IKE_SA_INIT request. If the VPN gateway supports this it will also send the DIFFERENT_TUNNEL_ADDRESS_SUPPORTED message back to the client in the IKE_SA_INIT response.

```
     Initiator                    Responder (VPN GW)
     ---------                    --------------------------

   (IKE_IP_I:500 -> IKE_IP_R:500)
   HDR(A,0), SAi1, KEi, Ni,   -->
   N(DIFFERENT_TUNNEL_ADDRESS_SUPPORTED)

                                (IKE_IP_R:500 -> IKE_IP_I:500)
                           <-- HDR(A,0),
                                N(DIFFERENT_TUNNEL_ADDRESS_SUPPORTED)
```

Once the Gateway gets the notification that the different tunnel address is supported by the endpoint, it can choose to assign the

tunnel address which is different than the address which is used for the IKEv2 signaling. Similarly the endpoint on getting the notification that the gateway supports the different tunnel address can chose to assign the different tunnel address. The following IKE_AUTH exchange describes this:

```
     Initiator                   Responder (VPN GW)
     ---------                   --------------------------
  (IKE_IP_I:500 -> IKE_IP_R:500)
  HDR(A,B), SK {IDi, [CERT,] [CERTREQ,]
  [IDr,]AUTH, SAi2, TSi, TSr, [N(TUNNEL_ADDRESS)]} -->

                            (IKE_IP_R:500 -> IKE_IP_I:500)
                       <-- HDR(A,B), SK {IDr, [CERT,] AUTH,
                            SAr2, TSi, TSr, [N(TUNNEL_ADDRESS)]}
```

The client will tell the TUNNEL-SRC-ADDRESS (client side) and the Gateway will tell the TUNNEL-DST-ADDRESS (gateway side). If only one side tells the different tunnel address, the IKE-address will be used as the other side's TUNNEL address.

4. IKEv2 CREATE_CHILD_SA exchange with different Tunnel Address

This section describes the use of different Tunnel Address mechanism during the CREATE_CHILD_SA exchange.

Please refer to section 3 for the DIFFERENT_TUNNEL_ADDRESS_SUPPORTED notification message during the IKE_SA_INIT exchange.

Once the Gateway gets the notification that the different tunnel address is supported by the endpoint, it can choose to assign the tunnel address which is different than the address which is used for the IKEv2 signaling during the CREATE_CHILD_SA request. Similarly the endpoint on getting the notification that the gateway supports the different tunnel address can chose to assign the different tunnel address. The following CREATE_CHILD_SA exchange describes this:

```
      Initiator                  Responder (VPN GW)
      ---------                  --------------------------
   (IKE_IP_I:500 -> IKE_IP_R:500)
   HDR(A,B), SK {{[N], SA, Ni, [KEi],
    TSi, TSr, [N(TUNNEL_ADDRESS)]} -->

                            (IKE_IP_R:500 -> IKE_IP_I:500)
                       <-- HDR(A,B), SK {SA, Nr, [KEr],
                            TSi, TSr, [N(TUNNEL_ADDRESS)]}
```

The client will tell the TUNNEL-SRC-ADDRESS (client side) and the Gateway will tell the TUNNEL-DST-ADDRESS (gateway side). If only one side tells the different tunnel address, the IKE-address will be used as the other side's TUNNEL address.

5. Usage Scenarios

5.1. IKEv2 signaling and the IPSEC tunnel mode traffic on different addresses

Currently it is not possible to separate the IKEv2 signaling and the IPSEC traffic on different IP addresses. There are applications where we would like to have different addresses for signaling and the IPSEC traffic coming to the gateway. One of these applications can be load balancing of IPSEC tunnels. In this model, all the IKEv2 signaling from the clients will go through the IKEv2 load Balancer to the selected gateway on a particular IP address, where as the IPSEC traffic from clients will go directly to the gateway (bypassing the load balancer) on different address. So in this case the signaling and the traffic will reach the selected Gateway at different addresses.

6. NAT Scenarios and Routing issues

In some scenarios, the network may contain NATs or stateful packet filters (for brevity, the rest of this document simply describes NATs). The NAT Traversal feature specified in [IKEv2] allows IKEv2 to work through NATs in many cases, and this draft will leverage this functionality.

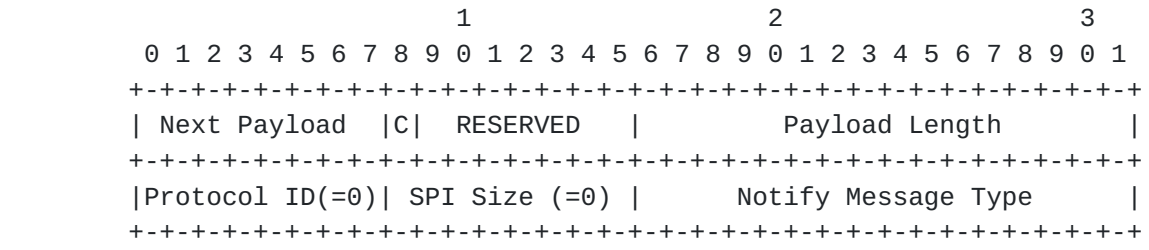
If the Gateway or the client determines that there is a NAT in front of them, they will not change the tunnel address and will keep the tunnel address same as the IKE address. If we try to solve this issue, it will add a lot of complexity to the [IKEv2] protocol.

The issues related to the routing of the IPSEC traffic between the negotiated Tunnel Addresses is beyond the scope of this document. The network operators need to take care of the routing between the VPN clients and the Gateway.

7. Alternate Tunnel address messages

7.1. DIFFERENT_TUNNEL_ADDRESS_SUPPORTED

The DIFFERENT_TUNNEL_ADDRESS_SUPPORTED payload is included in the initial IKE_SA_INIT request by the initiator or the IKE_SA_INIT_RESPONSE by responder to indicate support for the IKEv2 different tunnel address mechanism described in this document.



The 'Next Payload', 'Payload Length', 'Protocol ID', 'SPI Size' and the 'Notify Message Type' fields are the same as described in Section 3.10 of [2]. The 'SPI Size' field MUST be set to 0 to indicate that the SPI is not present in this message. The 'Protocol ID' MUST be set to 0, since the notification is not specific to a particular security association.

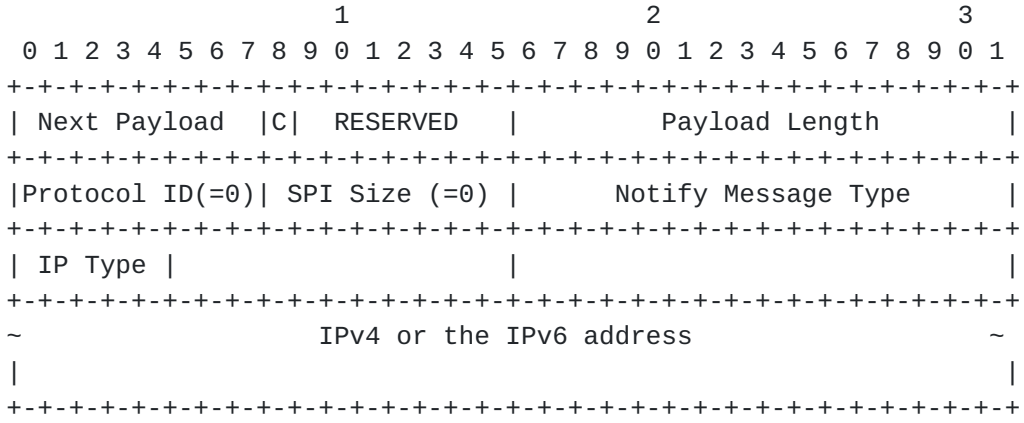
The 'Payload Length' field is set to the length in octets of the entire payload, including the generic payload header. The 'Notify Message Type' field is set to indicate the DIFFERENT_TUNNEL_ADDRESS_SUPPORTED Payload <value to be assigned by IANA>.

7.2. TUNNEL_ADDRESS

The TUNNEL_ADDRESS payload is included in an IKE_AUTH request or response and also in the CREATE_CHILD_SA request or response if the initiator or the responder wants to use the different address for the tunnel address (different than the address used for the IKEv2 signaling.

The message includes the IP address to be used for the tunnel src

(client) or the tunnel destination (gateway).



The 'Next Payload', 'Payload Length', 'Protocol ID', 'SPI Size' and the 'Notify Message Type' fields are the same as described in Section 3.10 of [2]. The 'SPI Size' field MUST be set to 0 to indicate that the SPI is not present in this message. The 'Protocol ID' MUST be set to (2) to indicate AH or (3) to indicate ESP, since the notification is specific to an IPSEC Security Associations. The 'Payload Length' field is set to the length in octets of the entire payload, including the generic payload header. 'Notify Message Type' field is set to indicate the TUNNEL_ADDRESS payload <value to be assigned by IANA>. The IP Type' field indicates the IP address type. The following values are valid in the TUNNEL ADDRESS payload.

1 - IPv4 address
2 - IPv6 address

The IPv4 address, the IPv6 address MUST be encoded as described in section 3.5 of [2].

8. IANA Considerations

This document defines two new IKEv2 Notification Message types as described in Section 7. The two Notify Message Types must be assigned values between 16396 and 40959.

- DIFFERENT_TUNNEL_ADDRESS_SUPPORTED
- TUNNEL_ADDRESS

This document creates a new namespace called the "IP Type". This is used to indicate the type of IP address being used.

1 - IPv4 Tunnel address
2 - IPv6 Tunnel address

Values '0', and 4-240 are reserved. New values can be allocated by Expert Review [9]. Values 241-255 are set aside for private use. A specification that extends this registry MUST also mention which of the new values are valid in which Notification payload.

9. Security Considerations

The main goals of this specification are to maintain the security offered by usual IKEv2 procedures and to counter any threats introduced by this draft in an appropriate manner. This section describes new security considerations introduced by this draft. See [IKEv2] for security considerations for IKEv2 in general.

9.1. Different Tunnel Addresses and Hijacking

The payloads relating to different tunnel addresses are encrypted, integrity protected, and replay protected using the IKE_SA. This assures that no one except the participants can, for instance, give a control message to use the different tunnel address.

However, as with normal IKEv2, the actual IP addresses in the IP header are not covered by the integrity protection. This means that a NAT between the parties (or an attacker acting as a NAT) can modify the addresses and cause incorrect tunnel header (outer) IP addresses to be used for IPsec SAs. The scope of this attack is limited mainly to denial of service because all traffic is protected using IPsec.

This attack can only be launched by on-path attackers that are capable of modifying IKEv2 messages carrying NAT detection indications (such as Dead Peer Detection messages). By modifying the IP header of these packets, the attackers can lead the peers to believe a new NAT or a changed NAT binding exists between them. The attack can continue as long as the attacker is on the path, modifying the IKEv2 messages.

10. Acknowledgements

Thanks to Bob Penfield and others for their input.

11. Informative References

11.1. Normative References

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

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

11.2. Informative References

[3] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[4] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[5] Haley, B., Devarapalli, V., Deng, H., and J. Kempf, "Mobility Header Home Agent Switch Message", RFC 5142, January 2008.

[6] Eronen, P. and J. Korhonen, "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol", RFC 4739, November 2006.

[7] Weniger, K. and F. Dupont, "IKEv2-based Home Agent Assignment In Mobile IPv6/NEMO Bootstrapping", draft-dupont-ikev2-haassign-02 (work in progress), January 2007.

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

[9] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[10] V. Devarapalli and K. Weniger, "Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5685, November 2009

Author's Address

Jitender Arora
Acme Packet
71 Third Ave.
Burlington, MA 01803, USA
Email: jarora@acmepacket.com

Prashant Kumar
Acme Packet
71 Third Ave.
Burlington, MA 01803, USA
Email: pkumar@acmepacket.com