IPSECME   D. Palomares (Ed)
Internet-Draft   D. Migault (Ed)
Intended status: Standards Track   Orange
Expires: August 16, 2014   February 12, 2014

IKEv2/IPsec Context Definition
draft-plmrs-ipsecme-ipsec-ikev2-context-definition-00

Abstract

IPsec/IKEv2 cluster are constituted of multiple nodes accessed via a single address by the end user. The traffic is then split between the nodes via specific IP load balancing policies. Once a session is assigned to a given node, IPsec makes it difficult to assign the session to another node. This makes management operations and transparent high availability for end users, difficult to perform within the cluster.

This document describes the contexts for IKEv2 and IPsec that MUST be transfered between two nodes so a session can be restored. This makes possible to tranfer an IPsec session transparently to the end user.

Status of This Memo

Copyright Notice

Table of Contents

1. Requirements notation

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. Introduction

Large clusters may take advantage of the multiple nodes to enhance the peer's Quality of Service by performing among others:

1) Fail-over with high availability.

2) Load balancing among cluster members.

3) Scalability for overloaded IPsec platforms.

4) Compatibility for IKEv2/IPsec context transfers among different constructors.

This document addresses transfer of an IPsec session between physically or virtually different nodes within an IKEv2/IPsec cluster. More specifically, the document describes the parameters that SHOULD be transmitted between the IPsec/IKEv2 nodes, so that IKEv2 and IPsec session can be restored on the other node.

Currently IPsec based services can hardly benefit from these features as IPsec Security Associations are bound to a single node and cannot be shared among different cluster members.

This draft describes the parameters that MUST be transferred in order to keep an IKEv2/IPsec session alive in conformance with the Security Architecture for the Internet Protocol [RFC4301] and the Internet Key Exchange (IKEv2) Protocol [RFC5996].

This includes information such as the cryptographic material, the algorithms and the IP addresses, among others parameters.

Note that IKEv2 and IPsec session do not need to be on the same node as IKEv2 and IPsec context are different. Note also that we do not specify in this document how the IKEv2 or IPsec context are transferred between one node to the other. This can be performed via a simple UDP session that MAY be IPsec protected, a SCP session [RFC4251] or using the context transfer protocol [RFC4067].

3. Terminology

This document uses the following terminology:

IKE_SA context: the set of parameters composing a single IKE Security Association. A bidirectional communication will need a pair of IKE_SAs, for incoming and outgoing IKE exchanges.

IPsec_SA Context: the set of parameters composing a single IPsec Security Association. A bidirectional communication will need a pair of IPsec_SAs for incoming and outgoing traffic.

ESP: acronym for Encapsulation Security Payload. This header is part of the IPsec Security Architecture to provide origin authenticity, integrity and confidentiality protection of packets.

4. IKEv2 Session parameters

Considering IKEv2/IPsec sessions as bidirectional, we provide a list of parameters needed to create the IKE_SAs, which are usually stored in the user-land:

1) Version of IKE: in this draft we only consider version 2.

2) The initiator flag and the responder flag for the IKE_SAs.

3) Local host address and remote host address (IPv4 or IPv6).

4) The IKE_SA’s SPI of both initiator and responder.

5) The initiator nonce , responder nonce and diffie-hellman secret.

6) The [SA] proposal including: encryption algorithm, length of the encryption key, integrity algorithm, length of the integrity key and the pseudo random function (prf) to generate the SKEYSEED.

7) The extensions and condition of the IKE_SA (NAT, EAP, MOBIKE...).

8) The IDs of the initiator and responder (ID_IPV4_ADDR, ID_IPV6_ADDR, ID_FQDN, ID_RFC822_ADDR, ID_DER_ASN1_DN, ID_DER_ASN1_GN or ID_KEY_ID).

5. IPsec Session parameters

Once the IKE_SAs are established for securing further IKEv2 exchanges, a pair of IPsec_SAs are negotiated in order to secure the traffic flow between nodes. The parameters of an IPsec_SA are usually stored within the kernel-land and user-land. The following is a list of the parameters needed to build an IPsec_SA:

1) Local host and remote host addresses (IPv4 or IPv6).

2) The inbound and outbound IPsec_SA Security Parameter Indexes (SPIs).

3) The sequence number counter.

4) The sequence number overflow flag.

5) The anti-replay window and the sequence number values.

6) IPsec mode: transport or tunnel mode.

7) The IPsec protocol ESP and/or AH, their encryption/integrity algorithms and the key lengths.

8) The SA Lifetime: a time interval or byte count after which an SA must be replaced with a new SA (and new SPI).

9) Path MTU: maximum size of an IPsec packet that can be transmitted without fragmentation.

10) Upperspec: upper-layer protocol to be used.

11) Source IP address and ports of the protected traffic.

12) Destination IP address and ports of the protected traffic.

6. IANA Considerations

There are no IANA consideration for this document.

7. Security Considerations

Transferring an IPsec context between different SG involves sending sensitive information through the network. These pieces of information MUST be sent to an authenticated node via a secure channel.

8. Acknowledgment

IPsec cluster management is a joint work between Orange, Universite Pierre et Marie Curie / LIP6 and Institut Telecom / Telcom SudParis.

We would like to thank Maryline Laurent and Tobias Guggemos for their advises.

9. References

9.1. Normative References

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

[RFC4251] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

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

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

9.2. Informative References

[RFC4067] Loughney, J., Nakhjiri, M., Perkins, C., and R. Koodli, "Context Transfer Protocol (CXTP)", RFC 4067, July 2005.

Appendix A. ANNEX A: Data structure example

Example of an IKEv2 data structure:

```
  typedef struct _IKEV2CONTEXT
           {
                bool *initiator;
                u_int32_t *ike_spi_i;
                u_int32_t *ike_spi_r;
                char *my_host;
                char *other_host;
                u_int16_t *enc_alg_ike;
                u_int16_t *enc_alg_ike_len;
                u_int16_t *int_alg_ike;
                u_int16_t *prf_alg;
                char *nonce_i;
                char *nonce_r;
                char *dh_secret
       } IKEV2CONTEXT;
```

Example of an IPsec session data structure:

```
     typedef struct _IPSECCONTEXT
               {
                    bool *initiator;
                    char *my_host;
                    char *other_host;
                    u_int8_t ipsec_mode;
                    u_int16_t *encr_alg_child;
                    u_int16_t *enc_alg_len_child;
                    u_int16_t *int_alg_child;
                    u_int32_t *enc_key_i;
                    u_int32_t *int_key_i;
                    u_int32_t *enc_key_o;
                    u_int32_t *int_key_o;
                    char *child_seq_i;
                    char *child_bit_i;
                    char *child_seq_o;
                    char *child_bit_o;
                    char *child_spi_i;
                    char *child_spi_o;
                    u_int16_t *ts_l_fromport;
                    u_int16_t *ts_l_toport;
                    u_int8_t *ts_l_type;
                    u_int8_t *ts_l_proto;
                    char *ts_l_fromaddress;
                    char *ts_l_toaddress;
                    u_int16_t *ts_r_fromport;
                    u_int16_t *ts_r_toport;
                    u_int8_t *ts_r_type;
                    u_int8_t *ts_r_proto;
                    char *ts_r_fromaddress;
                    char *ts_r_toaddress;
           } IPSECCONTEXT;
```

Appendix B. Document Change Log

[RFC Editor: This section is to be removed before publication]

-00: First version published.

Authors’ Addresses

Daniel Palomares
Orange
38 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

Phone: +33 1 45 29 51 16
Email: daniel.palomares@orange.com

Daniel Migault
Orange
38 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

Phone: +33 1 45 29 60 52
Email: daniel.migault@orange.com