IP Security Maintenance and Extensions (ipsecme)
Internet-Draft
Intended status: Informational
Created: June 26, 2013
Expires: December 26, 2013

A. Yamaya, Ed.
K. Ueki
T. Murai
Furukawa Network Solution Corp.
T. Ohya
NTT

June 26, 2013

simple VPN solution using Multi-point Security Association
draft-yamaya-ipsecme-mpsa-01.txt

Abstract

This document describes the over-lay network solution by utilizing dynamically established IPsec multi-point Security Association (SA) without individual connection.

Multi-point SA technology provides the simplified mechanism of the Auto Discovery and Configuration function.
This is applicable for any IPsec tunnels such as IPv4 over IPv4, IPv4 over IPv6, IPv6 over IPv4 and IPv6 over IPv6.

Table of Contents

1. Introduction

As described in the problem statement document[ad-vpn-problem], dynamic, secure and scalable system for establishing SAs is needed.

With multi-point SA, an endpoint automatically discovers other endpoint. In this draft, an endpoint means an inexpensive CPE, which can hardly establish large number of IPsec sessions simultaneously. The CPEs also share a multi-point SA within the same group, and there is no individual connection between them.

Scalability issue becomes serious in the service, such as triple play which requires large number of sessions at the same time. MPSA enables large scale simultaneous sessions even with inexpensive CPEs, and can avoid scalability issue.

The latency between CPEs can be minimized because of stateless shared multipoint SA, MPSA is suitable for video and voice services which is very sensitive to latency.

It can avoid the exhaustive configuration for CPEs/ gateways. No reconfiguration is needed when a new CPE is added, removed, or changed. It can avoid high load on the gateways.

1.1. Terminology

Multi-point SA - This is similar
to Dynamic Full Mesh topology described in [ad-vpn-problem];
direct connections exist in a hub and spoke manner, but only one SA
for data transfer is shared with all CPEs.

2. Motivation

There are two major topologies - Star topology and full-mesh topology -
to communicate securely on over-lay network by using IPsec.

Figure.1 shows star topology. The number of IPsec connection is the same as the number of CPEs (CPE). Authentication, Authorization and Accounting (AAA) of each CPE can be achieved on the gateway.

The problem of the star topology is all the traffic go through the gateway, then it causes high load and latency.

```
+---------------------------------------------+
|                IPsec Gateway                |
|                                             |
|    +--------------(A<->C)--------------+    |
|    | +---(A<->B)---+   +---(B<->C)---+ |    |
+---:|-|:-----------:|---|:-----------:|-|:---+
    :| |:           :|   |:           :| |:
    :| |:           :|   |:           :| |:
    :| |:           :|   |:           :| |:
+---:v-v:---+       :|   |:       +---:v-v:---+
|           |       :|   |:       |           |
|   CPE_A   |       :|   |:       |   CPE_C   |
|           |       :|   |:       |           |
+-----------+       :|   |:       +-----------+
                 +--:v---v:--+
                 |           |
                 |   CPE_B   |
                 |           |
                 +-----------+
```

Figure 1

Figure.2 shows Full-mesh topology. There is no gateways. Each CPE establishes IPsec connection independently. The latency on this topology is relatively low compared to star topology.

In large system, there are huge number ((N^2-N)/2) of IPsec connections.
AAA of each CPE is hard to manage in this topology.
Moreover, when a CPE is added, removed or changed, reconfiguration

is needed for all rest of the CPEs.

```
         +-----------+                     +-----------+
         |           |.....................|           |
         |   CPE_A   <-------(A<->C)------->  CPE_C    |
         |           |.....................|           |
         +---: ^ :---+                     +---: ^ :---+
             : | :                             : | :
             : | :        +-----------+        : | :
             : | :........|           |........: | :
             : +-(A<->B)-->  CPE_B    <--(B<->C)-+ :
             :............|           |............:
                          +-----------+
```

Figure 2

The solution in this document eliminates the problems listed above.
Figure 3 shows topology of multi-point SA.
Traffic between CPEs does not go through the gateway, low latency,
AAA of each CPE can be achieved, the number of
IPsec connection is almost same as star topology, and no reconfiguration
is needed for all the rest of CPEs even when a CPE is added,
removed or changed.

```
         +---------------------------------------------+
         |                IPsec Gateway                |
         |                                             |
         +---: | :------------: | :------------: | :---+
             : | :            : | :            : | :
             : | :            : | :            : | :
            ----------------------------------------- SA to distribute
             : | :            : | :            : | :  Multi-point SA
             : | :            : | :            : | :
         +---: v :---+    +---: v :---+    +---: v :---+
         |           |    |           |    |           |
         |   CPE_A   |    |   CPE_B   |    |   CPE_C   |
         |           |    |           |    |           |
         +--- ^ ^ ---+    +--- ^ ^ ---+    +--- ^ ^ ---+
         .....| |..............| |..............| |.....
              | |              | |              | |     \
              | +----(A<->B)---+ +---(B<->C)----+ |   Multi-point SA
              +--------------(A<->C)--------------+   for data transfer
         ................................................./
```

Figure 3

3. Procedure

3.1 Sequence

The multi-point SA capability of the remote host is determined by an exchange of Vendor ID payloads. In the IKE_SA_INIT exchange, the Vendor ID payload for this specification is sent if the multi-point SA is used.

```
    CPE                          Gateway
   -----------                        -----------
    HDR, SAi1, KEi, Ni, V(MPSA) -->

            <--    HDR, SAr1, KEr, Nr, V(MPSA), [CERTREQ]

                                          MPSA : multi-point SA
```

The initial exchange (including IKE_AUTH) is same as [IKEV2], other than Vendor ID payload included in IKE_SA_INIT.

After the initial exchange has finished successfully, a new INFORMATIONAL exchange is used to distribute multi-point SA to the CPE, with the Notify payload of MPSA_PUT that includes cryptographic algorithm, nonce, keying material, SPI and so on. Keys for multi-point SA is generated according to the contents of the Notify payload by the CPE. The response of the Notify payload has empty Encrypted payload.

```
    CPE                                  Gateway
   -----------                               -----------
                            <--    HDR, SK {N(MPSA_PUT)}

    HDR, SK {}             -->
```

3.2 Extended format

3.2.1 Vendor ID

This document defines a new Vendor ID. The content of the payload is described below.

   "multi-point SA"

3.2.2 MPSA_PUT

This document defines a new Notify Message Type MPSA_PUT. The Notify Message Type of MPSA_PUT is 40960. Notification Data of MPSA_PUT has a Proposal-substructure-like format. It consists of Transform-substructure-like structures that have following data.

```
Description                        Trans.  Reference
                                   Type
```

Encryption Algorithm (ENCR)	1	RFC5996
Pseudorandom Function (PRF)	2	RFC5996
Integrity Algorithm (INTEG)	3	RFC5996
Nonce (NONCE)	241	
SK_d (SKD)	242	
Lifetime (LIFE)	243	
Rollover time 1 (ROLL1)	244	
Rollover time 2 (ROLL2)	245	

- Nonce
  For Nonce, the Transform ID is 1.
  The attribute contains actual nonce value with attribute type 16384.
  The size of the Nonce Data is between 16 and 256 octets.

Name	Number
NONCE_NONCE	1

Attribute Type	Value	Attribute Format
Nonce Value	16384	TLV

- SK_d

  For SK_d, the Transform ID is 1.
  The attribute contains actual SK_d value with attribute type 16385.
  The length of SK_d Data is the preferred key length of the PRF.

Name	Number
SKD_SK_D	1

Attribute Type	Value	Attribute Format
SK_d Value	16385	TLV

- Lifetime

  For Lifetime, the Transform ID is 1.
  The attribute contains actual lifetime value with attribute type 16386.
  The length of Lifetime Value is 4 octets.
  Lifetime is stored in seconds as effective time of the multi-point SA.

Name	Number
LIFE_LIFETIME	1

Attribute Type	Value	Attribute Format
Lifetime Value	16386	TLV

- Rollover time 1

For Rollover time 1, the Transform ID is 1. The attribute contains actual rollover time 1 value with attribute type 16387. The length of Rollover time 1 Value is 4 octets. Rollover time 1 defines activation time delay for new outbound multi-point SA.

Name	Number
ROLL1_ROLLOVER1	1

Attribute Type	Value	Attribute Format
Rollover1 Value	16387	TLV

- Rollover time 2

For Rollover time 2, the Transform ID is 1. The attribute contains actual rollover time 2 value with attribute type 16388. The length of Rollover time 2 Value is 4 octets. Rollover time 2 defines deactivation time delay for old inbound multi-point SA.

Name	Number
ROLL2_ROLLOVER2	1

Attribute Type	Value	Attribute Format
Rollover2 Value	16388	TLV

Therefore, the format of the MPSA_PUT of the Notify Message is described below.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length        |
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Protocol ID  |   SPI Size    |      Notify Message Type      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Security Parameter Index (SPI)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| 0 (last) or 2 |   RESERVED    |         Proposal Length       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Proposal Num  |  Protocol ID  |    SPI Size   |Num  Transforms|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Security Parameter Index (SPI)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| 0 (last) or 3 |   RESERVED    |        Transform Length       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Transform Type |   RESERVED    |          Transform ID         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                      Transform Attributes                     ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| 0 (last) or 3 |   RESERVED    |        Transform Length       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Transform Type |   RESERVED    |          Transform ID         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                      Transform Attributes                     ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

~                                                               ~

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       0       |   RESERVED    |        Transform Length       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Transform Type |   RESERVED    |          Transform ID         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                      Transform Attributes                     ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The following example shows a N(MPSA_PUT) notification message. The SPIs in the Proposal-like and Tranform-like substructure are the same value. Following values are defined by the example.

```
 Protocol: ESP
 ENCR:     AES-CBC (256bits)
 PRF:      SHA-1
 INTEG:    HAMC-SHA-1-96
 NONCE:    241
 SKD:      242
```

```
 LIFE:     243
 ROLL1:    244
 ROLL2:    245
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+\
|     0 (last)  |C|  RESERVED   |         Payload Length        | \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  \
|    3 (ESP)    | SPI Size = 4  |           MPSA_PUT            | Notify
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  /
|                Security Parameter Index (SPI)                 | /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+<
|    0 (last)   |   RESERVED    |         Proposal Length       | \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Proposal-
| Prop Num = 1  |    3 (ESP)    | SPI Size = 4  |Num  Transforms|   like
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  /
|                Security Parameter Index (SPI)                 | /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+<
|       3       |   RESERVED    |        Transform Length       | \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  \
|   1 (ENCR)    |   RESERVED    |      12 (ENCR_AES_CBC)        | ENCR
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  /
|1|       14 (Key Length)       |            256                | /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+<
|       3       |   RESERVED    |        Transform Length       | \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ PRF
|    2 (PRF)    |   RESERVED    |      2 (PRF_HMAC_SHA1)        | /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+<
|       3       |   RESERVED    |        Transform Length       | \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ INTEG
|   3 (INTEG)   |   RESERVED    |    2 (AUTH_HMAC_SHA1_96)      | /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+<
|       3       |   RESERVED    |        Transform Length       | \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  \
|   241 (NONCE) |   RESERVED    |              1                |   \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+    \
|0|       16384 (Nonce)         |       Attribute Length        |   NONCE
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+    /
|                                                               |   /
~                            [Nonce]                            ~  /
|                                                               | /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+<
|       3       |   RESERVED    |        Transform Length       | \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  \
|   242 (SKD)   |   RESERVED    |              1                |   \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+    \
|0|       16385 (SK_d)          |       Attribute Length        |   SKD
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+    /
|                                                               |   /
~                            [SK_d]                             ~  /
|                                                               | /
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+<
|       3       |   RESERVED    |        Transform Length       | \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  \
|  243 (LIFE)   |   RESERVED    |               1               |   \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ LIFE
|0|       16386 (Lifetime)      |     Attribute Length = 4      |   /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  /
|                          [Lifetime]                           | /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+<
|       3       |   RESERVED    |        Transform Length       | \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  \
|  244 (ROLL1)  |   RESERVED    |               1               |   \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ROLL1
|0|       16386 (Lifetime)      |     Attribute Length = 4      |   /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  /
|                       [RolloverTime1]                         | /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+<
|       3       |   RESERVED    |        Transform Length       | \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  \
|  245 (ROLL2)  |   RESERVED    |               1               |   \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ROLL2
|0|       16386 (Lifetime)      |     Attribute Length = 4      |   /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  /
|                       [RolloverTime2]                         | /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+<
```

3.3 Multi-point SA Management

3.3.1 Gateway

Gateway generates a multi-point SA for a group before connecting to any CPEs.

After the initial exchanges have finished, Gateway distributes the same multi-point SA information to CPEs within the group by sending N(MPSA_PUT).

SPI and Nonce is generated similar way of [IKEv2].
SK_d is generated from random numbers similar to Nonce.

The same SPI value is stored to Notify payload and Proposal-like substructure.

The multi-point SA will not be negotiated between gateway and CPE, but will be notified from gateway to CPE one way.

Gateway initiates rekey before Lifetime expiration.
As the Lifetime, gateway notifies the effective time left of the multi-point SA.

3.3.2 CPE

After the initial exchange has finished, CPE obtains multi-point SA information by receiving N(MPSA_PUT) from gateway. The keys for the multi-point SA are generated in the same procedure described in [IKEv2], except Ni | Nr is replaced by Nonce.

Therefore, KEYMAT is derived by PRF listed below.

```
KEYMAT = prf+(SK_d, Nonce)
```

The multi-point SA is protected in a cryptographic manner by ENCR and INTEG which uses the generated keys.

The SPI value for the multi-point SA is the same of its in Notify message.

CPE uses the same multi-point SA as both inbound and outbound SAs.

CPE deletes both of inbound and outbound SA when Lifetime is expired.

Rollover time 1, 2 have no meaning when no old multi-point SA exists.

3.3.3 Rekeying

Rekeying should be finished before Lifetime expiration of current multi-point SA. Rekeying of multi-point SA will be performed as follows.

- Gateway generates a new multi-point SA
- Gateway distributes a new multi-point SA to all CPEs within the group
- CPE replaces the current multi-point SA to new one

CPE replaces multi-point SA using rollover method like [GDOI].

3.4 Forwarding

Each CPE sends and receives encapsulated packets using the multi-point SA.

The destination address of encapsulated packet will be determined with routing information, which can achieved by static configuration or route exchange mechanism such as BGP on encapsulated environment described in [MESH].

It is applicable for any IPsec tunnels such as IPv4 over IPv4, IPv4 over IPv6, IPv6 over IPv4 and IPv6 over IPv6.

4. Security Considerations

5. IANA Considerations

There is no new IANA considerations in this document.

6. References

6.1 Normative References

[IKEv2]
Charlie Kaufman, Paul Hoffman, Yoav Nir, Pasi Eronen
"Internet Key Exchange Protocol Version 2 (IKEv2)",
RFC5596, September 2010

6.2 Informative References

[GDOI] B. Weis, S. Rowles, T. Hardjono
"The Group Domain of Interpretation"
RFC6407, October 2011

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

[ad-vpn-problem]
S. Hanna, V. Manral "Auto Discovery VPN Problem Statement
and Requirements" draft-ietf-ipsecme-ad-vpn-problem-03,
"work in progress." December 17, 2012

7. Acknowledgments

Author's Addresses

Arifumi Yamaya
Furukawa Network Solution Corp.
5-1-9, Higashi-Yawata, Hiratsuka
Kanagawa 254-0016, JAPAN
Email: yamaya@fnsc.co.jp

Ken Ueki
Furukawa Network Solution Corp.
5-1-9, Higashi-Yawata, Hiratsuka
Kanagawa 254-0016, JAPAN
Email: ueki@fnsc.co.jp

Tomoki Murai
Furukawa Network Solution Corp.
5-1-9, Higashi-Yawata, Hiratsuka
Kanagawa 254-0016, JAPAN
Email: murai@fnsc.co.jp

Takafumi Ohya
NTT West Corp.
1-2-31, Sonezaki Kita-Ku
Osaka 530-0057, JAPAN
Email: t.ohya@rdc.west.ntt.co.jp