Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 10, 2009

Y. Xu
Tsinghua Univ.
P. Yang
Y. Ma
Hitachi (China) R&D Corporation
H. Deng
China Mobile
K. Xu
Tsinghua University

October 7, 2008

IKEv2 SA Synchronization for session resumption
draft-xu-ike-sa-sync-01

Status of this Memo

Abstract

It will take a long time and mass computation to do session resumption among IKE/IPsec gateways possibly maintaining huge numbers of IKEv2/IPsec SAs, when the serving gateway fails or over-loaded. The major reason is that the prcocedure of IKEv2 SA re-establishment will incur a time-consuming computation especially in the Diffie-Hellman exchange. In this draft, a new IKE security associations synchronization solution is proposed to do fast IKE SA session resumption by directly transferring the indexed IKE SA (named stub) from old gateway to new gateway, wherein the most expensive Diffie-Hellman calculation can be avoided. Without some time-consuming IKEv2 exchanges, the huge amount of IKE/IPsec SA session resumption procedures can be finished in a short time.

Table of Contents

1. Background

IKEv2 protocol which has been defined by [RFC4306] provides us a method to negotiate ipsec's key automatically between ipsec clients and gateway. Before negotiating ipsec's key, they should negotiate IKE's SA first. Usually, ipsec client sends IKE_INIT message to gateway with SAi1, KEi, Ni, then gateway chooses some proposal of SAi1 which come to the algorithm for encryption and decryption, also proposal for Diffie-Hellman, and then calculates the Diffie-Hellman, sends IKE_INIT respond message back to ipsec client. At this time, the most important keyring can be generated. After other IKE_AUTH exchange, The identity has verified. IKE SA has completely been established. The timing overhead of IKEv2 protocol, including some computation and signaling round-trips, is rather big especially when the Extensible Authentication Protocol (EAP) is used for third-party authentication. The picture below is the typical procedure for IKEv2 SA establishment.

```
    Initiator                          Responder
    -----------                        -----------
 HDR, SAi1, KEi, Ni      -->

                            < -- HDR, SAr1, KEr, Nr, [CERTREQ]

 HDR, SK {IDi, [CERT,]
 [CERTREQ,] [IDr,],AUTH,
 SAi2, TSi, TSr}         -->
                            < -- HDR, SK {IDr, [CERT,] AUTH,
                                 SAr2, TSi, TSr}
```

Figure 1: IKE_INIT and IKE_AUTH exchanges

The establishment of an IKE SA in the first two exchanges of IKEv2 procedure in [RFC4306] (especially Diffie-Hellman computation), is rather time-consuming. Normally, the IKEv2/IPsec gateway embodyment (like IPsec VPN gateway, Mobile IPv6 Home Agent, etc) keeps a large number of IKE/IPsec sessions. So in some scenarios (see Section 2), it will take a very time to re-establish all the IKE SA for session resumption of IKEv2/IPsec clients.

2. Application scenarios of IKEv2 Session Resumption

2.1. Scenario of IKEv2 Gateway fail

```
      IPsec                          old                    new/old
      client                         Gateway                gateway
       |                              |                        |
       |     IKE/IPsec SAs            |                        |
       |< ========================== >|                        |
       |                              |                        |
       |                              |                        |
       |                              O Fail of old GW         |
       |                              |                        |
       O detect the fail              |                        |
       | of old GW                    |                        |
       |                              |                        |
       |           new IKE init procedure                      |
       |< =================================================== >|
       |                              |                        |
       |           set up other child IPsec SAs                |
       |< =================================================== >|
       |                              |                        |
```

Figure 2: scenarios of IKEv2 Gateway fail

In this scenario, IPsec clients has established IKE/IPsec connections with old gateway with tunnel mode or transporation mode. Because of some reason, the old gateway may fail. In this case, IPsec client can know old gateway has failed(how to know gateway fail is out of our scope in this draft), and re-establish the IKEv2/IPsec sessions with the old gateway or another new gateway. While a large number of IPsec clients try to make the IKEv2/IPsec connections at the same moment, it will take a rather long time due to the reason mentioned in Section 1. And, the target gateway may have problem to response some clients in this case as well. The problem statement and goals for a failover solution are described in [Narayanan06].

2.2. Scenario of load-balance

```
      IPsec                          old                    new
      client                         Gateway                gateway
       |                              |                        |
       |     IKE/IPsec SAs            |                        |
       |< ========================== >|                        |
       |                              |                        |
       |                              |                        |
       |                              O overload of old GW     |
       |                              |                        |
       O detect the overload          |                        |
       | of old GW                    |                        |
       |                              |                        |
       |           new IKE init procedure                      |
       |< =================================================== >|
       |                              |                        |
       |           set up other child IPsec SAs                |
       |< =================================================== >|
       |                              |                        |
```

Figure 3: load-balance scenarios

In this scenario, after establishing IKE connections between IPsec clients and old gateway, the old gateway may be over-loading. then, some of the IPsec clients should stop the connection with old gateway and establish the connection with new gateway(how to know new gateway is also out of our scope). Again, while many IKE/IPsec sessions are transferred from old gateway to new gateway, it is a challenge to new gateway to re-establish bunch of IKE SAs at the same time.

3. Details on Proposed solution

3.1. Overview of the Proposed solution

In this section, a new data structure is named as "stub", which has the most important information of IKE SA. And gateway can use this data structure to accelerate the rebuilding of IKE SA. IKE_INIT message is extended with a new payload called IKE_SA_SYN. Since the gateway's IP address and SPI can uniquely index the stub of IKE SA, these two information are mandatory in the IKE_SA_SYN payload in order to retrieve the stub of IKE SA by the target gateway. The detailed data structure of Stub is introduced in Section 3.2.

The IKE SA session resumption procedure in this draft is depicted below:

```
Initiator                                    Responder
-----------                                  --------------
HDRGBP[not]SAr1, KEi, Ni, [SYN]   --->
                                   < --      HDR, Nr
```

Figure 4: IKE SA synchronization exchange

o While the IPsec client notices that it has to be transfer from old gateway to target gateway and want to pursue the fast session resumption, it sends IKE_INIT message with the SYN payload. The stub indexing information like old gateway IP address and old gateway's SPI shall be enclosed in the IKE SYN payload.

o Upon receiving the IKE_INIT message with the IKE_SA_SYN payload, the target gateway uses the information inside to retrieve the the stub of previous IKE SA in the stub bank. if the retrieved stub is qualified for IKE SA re-building, the target gateway will choose the new SPI, derive the new set of keyring and re-establish the IKE session for the related client. Lastly, it sends IKE_INIT response with new SPI in the IKEv2 header and Nr. The new IKE_SA has been re-established successfully.

If the taget gateway does not support IKE_SA_SYN or not find the proper stub, it can establish IKE SA by normal IKE_INIT and IKE_AUTH exchanges as specified in [RFC4306], or just drop the packet based on the local policy configured by network operator.

The stub can be stored in an independent stub bank, co-located with target gateway or even co-located with the corresponding IPsec client. This is discussed in Section 3.5. However, the case of stub co-located with IPsec client is only optional in this draft.

3.2. data structure of stub

the stub data structure should conclude all these informations.

- IDi, IDr.
- SPIi, SPIr.
- SAr (the accepted proposal).
- SK_d_old.
- shared secret.
- old gateway's ip address.
- lifetime

In the data structure of stub, the old gateway's ip address and SPI are used as the index for retrieval of stub.

SAr have the encrypt and decrypt algorithm, and shared secrect is the DH exchange's result, we can calculate the IKE SA's keyring as rekey process. It will be very quick.

3.3. Consideration on building IKE SA in session resumption

After the stub index has been presented by IKE client in the gateway, it will retrieve the stub from the stub bank. The way to get the stub from the stub bank can be found in Section 3.4.

As shown in Section 3.2, IDi, SA value can be obtained directly from the retrieved stub. The target gateway shall choose the new SPIr (called SPIr_new in this draft) for the key derivation of session resumption. The nounce values, Ni and Nr, are from the current IKE SYNC exchange.

So, the new value of SKEYSEED is calculated as below (SK_d_old value is from the stub):

```
SKEYSEED = prf (SK_d_old, Ni | Nr)
```

And the keyring set are derived by the way of generic IKEv2

```
{SK_d | SK_ai | SK_ar | SK_ei | SK_er | SK_pi | SK_pr } = prf+
                        (SKEYSEED, Ni | Nr | SPIi | SPIr_new )
```

The prf (pseudo-random function) of the cryptographic algorithms is specified in the SA value of stub.

3.4. Consideration on Stub handling

1) generation

After IKE SA has been established(after first two exchanges), the IKE/IPsec gateway extracts the stub from IKE SA.

2) propagation

After extracted from IKE SA, stubs should be updated to infrastructure such as stub bank. The stub bank can be independent entity in the network or co-located with the gateways (see Section 3.5).

3) Retrieve

The gateway can use the the old gateway's ip address and spi can index the unique stub.

4) Expire

The stub may be invalid when the lifetime expires. The value of lifetime is recommended to be same as the one in the IKE SA. The gateway may set different lifetime in stub.

5) Delete

When the IKEv2/IPsec session is deleted, the gateway shall delete the related stubs in the stub bank.

The following signaling shall be supported by IKE/IPsec gateways to communicate with Stub bank.

o Initiate Stub:

Gateway initiates the stub in the stub bank once new stub has been established. The index shall at least include the gateway's IP address and SPI.

o Update Stub:

Gateway updates its stub to infrastructure once the related IKE SA has been changed

o GET Stub:

Gateway uses this message to receives stub by the information in IKE_SA SYN payload from IKE client.

o Download Stub:

The stub bank can use this message to push the stubs to gateway.

o Delete Stub:

The Gateway can delete the stubs while the related IKE SAs are no longer available.

3.5. Consideration on location of Stub

1. Centralized infrastructure

```
    IPsec                  old        Target          stub
    client                 GW         GW              bank
       |                     |        |                 |
       |      IKE/IPsec      |        |                 |
       |< ================= >|        |    Update Stub  |
       |                     | ------------------------>|
       |                     o  Fail  |                 |
       |                     |        |                 |
       |         HDR,SAr1,KEi,Ni,SYN  |                 |
       |----------------------------->|  GET Stub       |
       |                     |        |---------------->|
       |                     |        |  Download Stub  |
       |                     |        |< ---------------|
       |      HDR,Nr         |        |                 |
       |< --------------------------- |                 |
       |                     |        |                 |
```

Figure 5: centralized structure

This proposal has a centralized Stub Bank server, gateway doesn't need local stub database.

a) After IKE connection has been established, old gateway set up the stub to stub bank.

b) Once the fast session resumption is started, IPsec client sends IKE_INIT with SYN payload.

c) When the target gateway receives IKE_INIT with SYN payload, it asks Stub Bank for stub via GET Stub signaling.

d) stub bank push proper stub to target gateway.

e) Target gateway gets the stub and rebuild IKE SA, then send HDR, Nr to Notify IPsec client that the new IKE SA has been set up by IKE SYNC session resumption.

2. Distributed infrastructure

```
    IPsec                  Target                Old GW
    client                 gateway                Stub
       |                     |                     |
       |  HDR,SAr1,KEi,Ni,SYN|     Update Stub     |
       | ------------------->| < ------------------|
       | < ------------------|                     |
       |      HDR,Nr         |                     |
```

Figure 6: distributed structure

This structure doesn't have centralized Stub Bank, and all gateway must have local stub database. if there is stub in local database, it will find the stub in local database, otherwise, it will GET the stub from other gateways.

a) After IKE connection has been established, old gateway initiates the stub to the potential target gateway.

b) Once session resumption is initiated, IPsec client send IKE_INIT with SYN payload.

c) Target gateway finds the proper stub and rebuild IKE SA, then send HDR, Nr to IPsec client.

Gateway has to store stubs in distributed structure, but it seems more simple than centralized structure. Also, these two proposals can mix together, other gateway also can be Stub Bank.

3. Full distributed in IKEv2/IPsec Client

There is also the possibility that the Gateway or Stub bank push the stub to the corresponding client. During the session resumption process, the target gateway can have another option to retrieve the stub from the corresponding client by the way specified in Section 3.4. But, this way of stub co-located with IPsec client is ONLY OPTIONAL. if the operator wants to use this case, the stub MUST be protected perfectly by strong encryption and integrity protection. So, in this draft, it is only optional to co-locate the stub in the client.

3.6. When should Gateways download/update Stub

Because of the stub is not sensitive with time, the gateways assemble the stub messages to reduce the message number in initiate event.

The single gateway can get many stubs at a time in download event.

The gateway may also update the stubs in bundles whenever it was

thought to be necessary

3.7. Related new messages

1)IKE_SA_SYN Payload format

```
                        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        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         GateWay's SPI                         |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         GateWay's IP Address                  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

C bit is the direction of this message.

2) Stub related signaling

Header Format

```
                        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|       type   |         Payload Length          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

type	number
Init	0x01
update	0x02
get	0x03
download	0x04
delete	0x05
reserved	0x00

```
                        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|   RESERVED   |         Payload Length          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                         PAYLOAD CONTENT                       |
   ~                                                               ~
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

4. Modification on the base IKEv2 protocol

As the core principle of this draft, the base IKEv2 protocol should be changed as little as possible. In the proposal, three aspects require slight modification on IKEv2 protocol in [RFC4306]

1) new IKE payload in the IKE_INIT message: IKE_SA_SYN

2) Modification on the state machine

IPsec client can send generic IKE_INIT message with SYN payload, if it decides to use the session resumption. Upon receiving IKE_INIT response only with the Nr and SPIr_new, it will calculate the new IKE SA as IKE SA rekey. And set state to IKE SA has been established. if the session resumption can not be accepted by the target gateway, the client will receive the usual IKE_INIT response as in [RFC4306] and continue the usual IKE_AUTH procedure afterwards

The target gateway, once receives IKE_SA_SYN payload, will firstly find the proper stub. if the stub can be found successfully, it will follow the session resumption proecedure as specified in this draft: re-establish IKE SA, send IKE_INIT respond with Nr only to ipsec client, and set state to IKE SA has been established. if the session resumption can not be accepted by target gateway, it just follows the usual IKEv2 initiation procedure as in [RFC4306]

3) The gateway should support the Stub related functions as specified in Section 3.4

5. Security Considerations

the security framework of IKEv2 protocol will not be compromised in this solution.

1) The stub index (Old gateway's IP address and SPI) in IKE_SA_SYN is a light-weighted information, which can be transported without encryption. And it relies on IKE_INIT message to handle the replay protection and DoS attack.

2) The Gateway can use SAr1, KEi to verify the identity, such as ID property.

3) Even if the index is right and IPsec client cannot rebuild IKE_SA because of some reason, the newly re-built IKE SA in gateway will be deleted after somewhile.

4) In the case of stub co-located with IPsec Client, the stub MUST be perfected protected to prevent the malicious attackers from cracking the stub, if they can obtain the stub on the network. Actually, even if the stub is strongly encrypted, there still has the risk. With the development of harware in accord with the Moore's Law, the capability of computing equipment will be increased step by step. Sometime, somehow, the brutal force decryption of the stub encryption method may be possible. And, there is also posibility that the currently safe encryption algorithm may be proved to be mathematically solvable. So, all in all, it is only optional to tranport the stub on the untrusted network, even if it can be protected strongly.

6. Conclusion

In this draft, a new solution is proposed to do IKE SA synchrinization for quick session resumption of IKE SA. With the extension of IKE_SA_SYNC payload in IKE_INIT message, it can remove the most time-consuming IKEv2 exchanges to re-build the IKE SA, which makes it much faster to transfer millions of IKE sessions from old gateway to target gateway. And the proposal in this draft will just slightly modify the base IKEv2 protocol with a new logical IKE SA Stub bank in the network.

7. Normative References

[Narayanan06]
Narayanan, V., "IPsec Gateway Failover and Redundancy Problem Statement and Goals", draft-vidya-ipsec-failover-ps-00.txt (work in progress), December 2006.

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

[Sheffer07]
Xie, Y., "Stateless Session Resumption for the IKE Protocol", draft-sheffer-ike-session-resumption-00.txt (work in progress), January 2007.

Authors' Addresses

Yan Xu
Tsinghua Univ.
Department of Computer Science
Tsinghua University
Haidian District
Beijing, 100088
P.R. China

Email: xydkl@163.com

Peng Yang
Hitachi (China) R&D Corporation
301, North Wing, Tower C Raycom Infotech Park
2 kexueyuan Nanlu
Haidian District
Beijing, 100080
P.R. China

Phone: +861082862918(ext.)328
Email: peng.yang.chn@gmail.com

Yuanchen Ma
Hitachi (China) R&D Corporation
301, North Wing, Tower C Raycom Infotech Park
2 kexueyuan Nanlu
Haidian District
Beijing, 100080
P.R. China

Phone: +861082862918(ext.)327
Email: ycma@hitachi.cn

Hui Deng
China Mobile
53A,Xibianmennei Ave.,
Xuanwu District,
Beijing 100053
China

Email: denghui@chinamobile.com

Ke Xu
Tsinghua University
Department of Computer Science
Tsinghua University
Haidian District
Beijing, 100088
P.R. China

Email: xuke@mail.tsinghua.edu.cn

Full Copyright Statement

Intellectual Property