Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 19, 2007

V. Narayanan, Ed.
Qualcomm, Inc.

May 18, 2007

IPsec Gateway Failover and Redundancy - Problem Statement and Goals
draft-vidya-ipsec-failover-ps-02

Status of this Memo

Copyright Notice

Abstract

Recovering from failure of IPsec gateways maintaining large numbers of SAs may take several minutes, if they need to re-establish the IPsec SAs by re-running the key management protocol, IKEv2. A similar problem arises in the event of a network outage resulting in the failure of several gateways and servers. The latency involved in this approach is significant, leading to a need for a faster and yet secure failover solution. This document describes the problem statement and the goals for an IPsec/IKEv2 gateway failover/

redundancy solution.

Table of Contents

1. Contributors

This document reflects contributions from and active discussions among the following individuals (in alphabetical order):

Lakshminath Dondeti (ldondeti@qualcomm.com)

Paul Hoffman (paul.hoffman@vpnc.org)

Tero Kivinen (kivinen@iki.fi)

Gregory Lebovitz (gregory.ietf@gmail.com)

Marcus Leech (mleech@nortel.com)

Cheryl Madson (cmadson@cisco.com)

Michael Richardson (mcr@sandelman.ottawa.on.ca)

Sheela Rowles (srowles@cisco.com)

Yaron Sheffer (yaronf@checkpoint.com)

Marcus Stenberg (mstenber@cisco.com)

Brian Weis (bew@cisco.com)

2. Introduction

The IKEv2 protocol, while more efficient and involves fewer round trips compared to its predecessor is quite computationally intensive, especially when entity authentication is by way of public-key based certificates. IKEv2 also needs 2-3 roundtrips when using PSKs or public keys for authentication and 4 or more roundtrips when EAP is used for client authentication. Thus, the process of setting up IPsec SAs is an expensive process, in terms of the number of messages exchanged between the initiator and responder.

Aside from the number of messages, IKEv2 also uses Diffie-Hellman for key negotiation. Network or gateway failures that result in a large number of clients reconnecting to a gateway will potentially lead to expensive computation on the gateway due to too many D-H exchanges within a short time span.

When an IPsec entity has a large number of SAs with various other endpoints, establishing all the SAs again upon a failure recovery condition takes a long time. Examples of entities that manage a

large number of IPsec SAs include IPsec remote access gateways, and application servers that use IPsec for protection of signaling traffic. For efficient recovery from gateway or server failure, it might make sense to allow those entities to maintain copies of IPsec and IKEv2 state (SAD, SPD, and associated state) on other gateways (for stateful operation) or on the client itself (for stateless operation). Either the recovered IPsec entity or other entities in the gateway pool may retrieve the stored IPsec and IKEv2 state for faster recovery.

There are a number of proprietary solutions for some part of this problem in the industry, however, those solutions do not interoperate. Applications that need IPsec failover capability, such as Mobile IPv6 have solutions under development for interoperable Home Agent (HA) failover. Without interoperable (client to server and server to server) IPsec failover capability, Home Agent failover solutions are incomplete. Thus, there is a need for an interoperable means of performing SA uploads and retrieval so that such IPsec redundancy can be implemented in an interoperable fashion.

3. 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 RFC 2119 [1].

This document uses terminology defined in [2], [3], and [4]. In addition, this document uses the following terms:

4. Motivation and Background

This work is motivated by the use of IPsec in 3G networks, where the protocols used are often optimized for efficient, low overhead, low latency operation. As will be noted from the rest of this document, this does not mean that a solution developed will only be applicable for use in such 3G networks. The intent is to develop a solution that will be applicable for any entities using IKEv2/IPsec. This section provides details on the motivation and background that will help understand the problem statement and goals that follow.

4.1. Use of IPsec in 3G Networks

A high level view of a 3G network with the various IPsec components is shown in Figure 1.

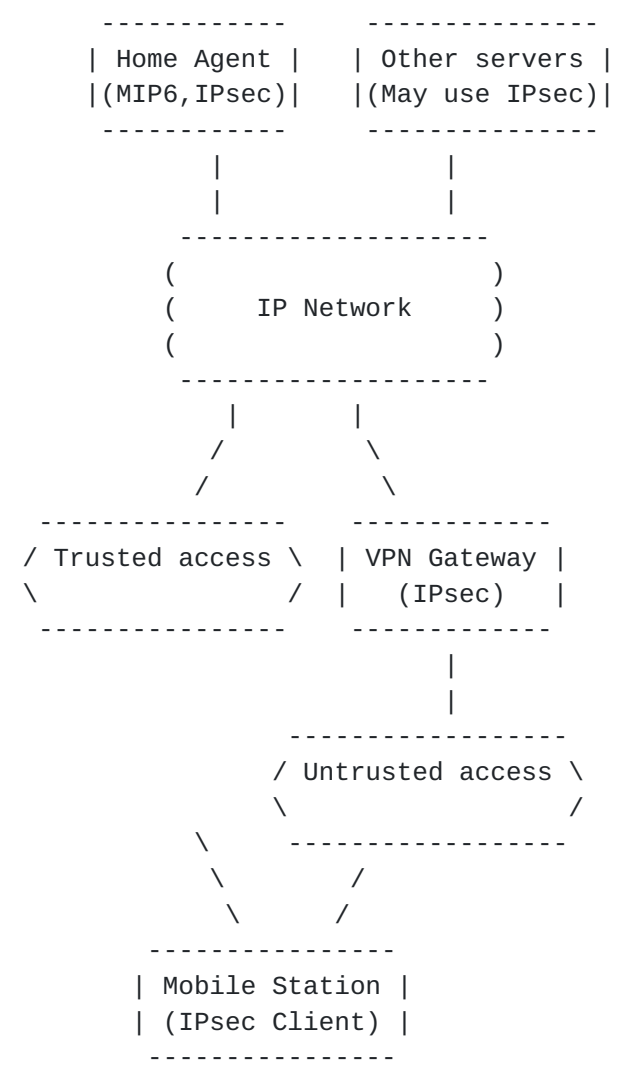

Figure 1: High Level Network View with IPsec Components

There are multiple uses of IPsec being considered in next generation 3G networks. One is the use of IPsec in untrusted access networks - this is much like a remote access VPN, with a VPN gateway placed in the network to provide secure connectivity to mobile devices over an untrusted network. The second is the use of IPsec for Mobile IPv6 (MIP6) - here, the MIP6 signaling is protected using IPsec, as required by MIP6, between the mobile node and the Home Agent (HA). Additionally, data tunneled through the Home Agent may also be protected using IPsec. In both these cases, IKEv2 is the mode of establishing the IPsec SA and EAP is often used in IKEv2 for client authentication.

A third use of IPsec is in the IP Multimedia Subsystem (IMS) - however, IKEv2 is not used to set up the IPsec SA for use in IMS and

hence, that use is not considered in this document. It should be noted that these may only be a subset of the IPsec use cases; this document applies to any use of IPsec that uses IKEv2 for SA establishment.

In all these cases, the execution of IKEv2 (especially with EAP for client authentication) takes up a number of message exchanges and reasonable computational expense. When executed once upon power up, it may not be a significant concern. However, if IKEv2/EAP needs to be executed during handoffs, it often adds an unacceptable handoff latency. Further, upon failure of the network or the IPsec gateway, there is significant time needed to bring all the clients back in service.

Distributed network elements to which the clients can connect using IPsec allow distributed failovers without the need for a fully reduandant IPsec gateway. Even when a fully redundant IPsec gateway is used, the ability to failover to distributed gateways provides better site-level redundancy.

4.1.1. Mobile IPv6 in 3G Networks and IPsec State Related Concerns

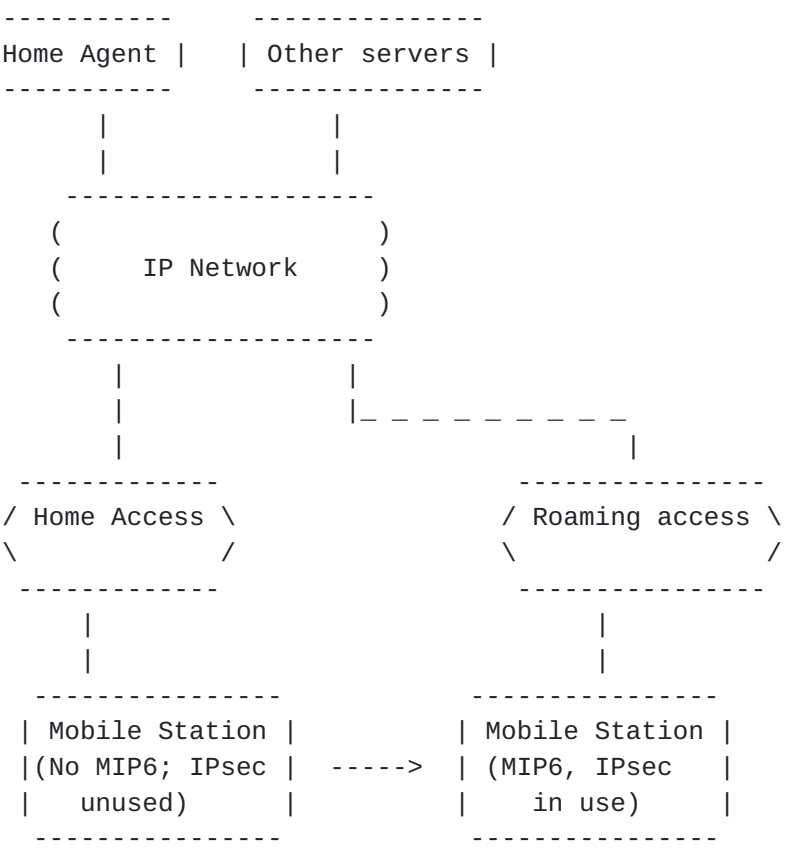

Figure 2: Mobile IPv6 with Home and Roaming Networks

One potential use of MIP6 in 3G networks involves using the protocol only when the mobile node roams outside of the its home network. This is shown in Figure 2. There is a need to keep the handoff upon roaming seamless and hence, this makes the setting up of IPsec SAs upon roaming undesirable. It is also not always feasible to predict roaming well ahead of time, sufficiently enough to proactively set up an IPsec SA. For this reason, it is better to set up the SAs while the mobile node is still on the home network (for e.g., upon first attachment to the network).

However, it is also the case that device roaming is unpredictable - so, if the Home Agent is required to maintain all the IPsec SAs for all the mobile nodes, that is a significant waste of resources on the Home Agent, given that it is maintaining state for several devices that may never roam. Hence, establishing the IPsec SA, losing the state on the Home Agent, and allowing resumption of state when needed is a more scalable approach to handling the scenario.

This case, while does not constitute a true failure of any kind, can be viewed as an instance where the network lost the state meant for the client. In such circumstances, any stateless failover mechanisms defined can be used to quickly resume the IPsec SA when the mobile device roams and actually needs to use it.

4.2. Mobile IPv6 Home Agent Reliability and IPsec Failover

There are ongoing efforts to standardize Mobile IP Home Agent reliability [5] mechanisms for interoperable MIP6 failovers. The scope of that work addresses having distributed home agents that share MIP6 state. IPsec state sharing is not assumed by the work, although some IPsec state may be shared across the gateways. For this work, it is assumed that the home agents will have different IP addresses, although, the client IP addresses will be preserved after failover. If the IPsec state is perfectly synchronized among the different home agents, it may be feasible to have a failover that is transparent to the clients from an IPsec perspective. Note that the failover is not exactly transparent from a Mobile IP perspective, due to the change in Home Agent IP address. However, per packet synchronization of IPsec state is very hard to achieve, especially across distributed entities and hence, a need for client involved IPsec failover also becomes essential in that case.

In all the cases described above, the resumption of IKEv2/IPsec state needs to happen with minimal latency to avoid longer resumption times for applications in progress on the clients.

5. Applicability and Problem Statement

There are at least two cases where fast recovery from failure of an IPsec entity is applicable.

IPsec Gateways -- The first case is that of an IPsec remote access gateway managing tunnel mode SAs with clients. The gateway may be enforcing access control to an enterprise network; this is the typical remote access use case. The gateway could also be enforcing service provider network access control. In that case, clients typically use EAP over IKEv2 to establish an IPsec session with a network access gateway. In either IPsec Gateway use case, the IPsec traffic itself flows from the VPN clients or Initiators to the VPN gateway; the gateway decapsulates the IPsec packets and forwards the cleartext packets based on inner IP headers. In the reverse direction, the VPN gateway uses the security policy database (SPD) or associated caches as per RFC4301, to lookup the relevant IPsec SA, encapsulates the packets and sends to the appropriate VPN client.

Servers -- The second use is that of an IPsec entity acting as a server for an application such as Mobile IP. In these cases, Mobile IP messages are protected using IPsec. Each Mobile IP Home Agent (HA) maintains a large number of transport or tunnel mode IPsec sessions with their respective clients. In this case, IPsec protected signaling messages are sent end-to-end, between Mobile IP client and HA, respectively.

In the security gateway mode, while there may be multiple security gateways serving a number of remote endpoints, a given remote endpoint is served by one security gateway. For instance, an IPsec VPN client typically maintains one or more SAs for remote access with one VPN gateway. However, when the serving gateway fails, it is desirable for one of the other gateways to seamlessly take over and serve the clients affected by the failure. In some deployments, there may be a backup gateway that can take over for the primary in case of a failure. Such gateways may be running a VRRP-like protocol to actually share the gateway IP address as known to the clients. In other deployments, a cluster of gateways may load balance to serve a number of clients. In such a case, one or more of the gateways in the cluster may take over clients associated with another gateway in the cluster in the event of a failure.

When IPsec is used for protection of signaling between an application client and server, server redundancy is often an important consideration. As in the gateway model, it is necessary for another server to be able to seamlessly take over clients being served by a failed server.

In cases of gateway or server failures, it may also be that the clients re-attach to the same gateway or server after recovery of the entity. The failover procedures must be able to support that type of recovery.

In addition to server failures, massive network failures of a short duration (minutes), followed by network recovery are also a concern. The network failure results in all clients being disconnected first (e.g. because of dead-peer detection), and then simultaneously attempting to reconnect. This can be classified as a subset of the gateway failure case for the purpose of this effort.

In all these cases outlined above, it is feasible to perform secure IPsec and IKEv2 state transfer across endpoints to provide smoother failure recovery. Today, such redundancy operations are performed in a vendor specific manner and are not interoperable. Also, lack of client involvement implies a failover mode that is transparent to the client. However, in the above cases, the failover may not always be transparent to the client and hence, an interoperable mechanism becomes very important.

5.1. Failover Cases

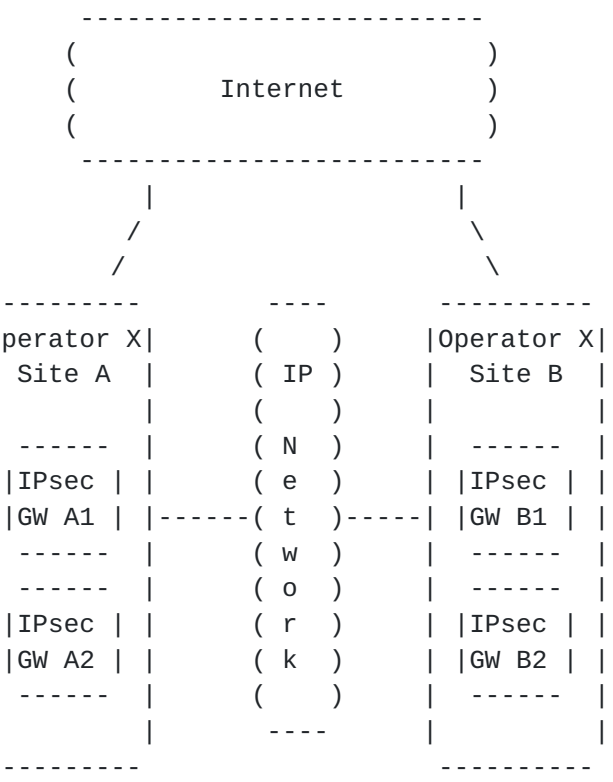

Figure 3: Various IPsec Entities in the Network

Figure 3 shows the various possible IPsec gateways that may be present in an operator's network. This figure shows a two-site operator network, each of which may have multiple IPsec gateways. Even though the term "IPsec gateway" has been used in the figure, it is also representative of any application server serving as an IPsec endpoint. The following are applicable failover cases under consideration.

1. Intra-site gateways with no direct gateway-to-gateway state synchronization mechanisms: In this case, the IPsec state is either partially available (e.g., no per packet state synchronization, but, the IKE SA is available, etc.) or not available at all. However, this does not restrict any state synchronization of other applications (e.g., the Mobile IP state may still be fully sychronized). This would be a case where IPsec Gateway A2 or B2 is acting as the backup gateway for IPsec Gateway A1 or B1 respectively in Figure 3.

2. Inter-site gateways that are geographically distributed: It is assumed that complete IPsec state synchronization across inter-site gateways is either complicated or impractical. This again does not rule of synchronization of other state such as Mobile IP state. This would be a case where IPsec Gateway B1 or B2 is acting as the backup gateway for IPsec Gateway A1 or A2 or vice-versa in Figure 3.

3. Gateway reboots: This is the case of clients attaching to the same gateway after it has recovered from a failure. Often, the gateway has lost the relevant IPsec state in such cases. This would be a case where any single IPsec Gateway in Figure 3 recovers from a failure and has clients connecting to it again.

6. IPsec Failover Redundancy Solution Goals

The following are goals for the IPsec Failover Redundancy solution. Note that the motivation for this effort is to develop mechanisms and perhaps protocols to facilitate failover capabilities. It is plausible that the design facilitates features such as load balancing, but additional signaling or protocol design to facilitate load balancing exclusively is outside the scope of this effort.

1. Distributed Failover Mechanism: Gateways may be located at different sites and may not share the same IP address or have the same view of the network. For instance, the various distributed gateways may be connected to different backend elements such as

EAP servers, DHCP servers, etc. A failover mechanism must be able to allow such distributed gateways to take over the clients associated with a failed gateway. The idea here is that there is no need for a fully redundant gateway that only starts functioning in the event of a failure. It is more cost-effective to allow such failover to distributed gateways that may be functional on their own, serving other clients. The temporary increase in load on some gateways in the system may be acceptable to many deployments in the event of a failure. Such a mechanism across distributed gateways may also be used for client handoff to other gateways due to other reasons, e.g., load balancing. Gateways located on the same link with the same view of the network may be viewed as a subset.

2. Client Involvement: Given that the gateways may be distributed, the failover is not intended to be transparent to the client. There may be times when the client, from its perspective, sees the gateway as unavailable and therefore needs to take some action to use a new gateway. The goal is to allow the option for the client to initiate the switch to a different gateway. In some cases, such as the Mobile IPv6 Home Agent reliability process, the Home Agent, acting as the IPsec gateway, may initiate the switch. This is due to the fact that the MIP6 Home Agent reliability procedures would allow a new Home Agent to detect the failure of an old Home Agent and trigger communication with its clients.

3. Low Latency failover: One of the major goals is to allow a low latency failover, without having to re-establish all the IKEv2 and IPsec state all over again. The bottleneck here is the new IPsec gateway trying to handle a flood of IKEv2 exchanges upon a failover. Further, for applications such as Mobile IPv6 that use IKEv2/IPsec for securing the signaling, re-establishment of IKEv2 often adds unacceptable latencies. Ideally, a mechanism that does not need any new messages to exclusively support failover is desired. In general, the goal is to have significantly lower latency and to incur a lower computational overhead than a regular IKEv2 exchange. In cases where EAP is used for client authentication in IKEv2, the failover should not require EAP authentication, to avoid AAA overloading and possible user interaction. This may mean that any attributes returned from the AAA server as a result of EAP must also be stored as part of the state, if those are required for IPsec operation.

4. Application Usage of IPsec: When IPsec is used to protect other protocols, the extent of failover interoperability that can be expected by such protocols greatly hinge on the interoperability of IPsec failover mechanisms. For e.g., Mobile IP Home Agent

reliability [5] mechanisms are intended to be standardized for interoperability. However, it is incomplete without IPsec failover. So, it is important to allow applications that use IPsec to take advantage of the IPsec failover mechanism. It is not expected that the IPsec failover solution will address this, but a guidance needs to be provided to allow application specifications to specify the appropriate interface/interaction needed (e.g., if synchronization between application state and IPsec state is needed).

5. Interoperability: Client-gateway and gateway-gateway interoperability is required. Note that the gateway-gateway interoperability does not refer to any full SA state synchronization mechanisms across gateways. Interoperability across gateways is, however, needed from the perspective of having a standard state format that multi-vendor gateways would be able to use for failover, for example.

6. Stateless Gateway Operation: The IPsec failover mechanism should specify a mode of operation that will allow the backup gateways to not have to maintain state for clients it is not serving. A gateway must need to acquire and store state for a client that is otherwise served by a different gateway, only when a failover occurs or during a temporary service interruption with the client's old gateway. This will allow for better scalability of the solution, since a given gateway only needs to store state for clients that are being served by it. This requires for an equally secure means of storing state in the clients and allowing the client to present it to the gateway for recovery.

7. Support for IPsec transport and tunnel modes: As noted in the applicability section of this document, the IPsec infrastructure endpoint may either be an IPsec VPN gateway employing tunnel mode SAs with the client or an application server that uses IPsec transport or tunnel mode to protect signaling exchanges with the client. Hence, a solution developed for failover must support failover of both transport and tunnel mode SAs.

7. Security Considerations

This document provides the problem description and goals for an IPsec failover solution. The solution must ensure secure operation and there are several important points to consider for that. We highlight a few of the important ones below :

- First, any SA storage and retrieval mechanisms specified between the backend entities must be protected with a secure channel that

has the following properties: confidentiality, integrity protection, and replay protection.

- In a client-server model, where the client always initiates the secure communication, the client is always the IKEv2 initiator. Solutions for failover in such cases, may allow the client to find the new gateway IP address through external means. Subsequently, the client must be able to verify that the new gateway possesses the IKEv2 key material. A client should be able to initiate a new IKEv2 SA with one or more auxiliary gateways without interrupting a connection to the currently used primary gateway. The client must consider the new gateway as a provisional one until it has verified a new gateway is the appropriate replacement for the primary gateway.

- Any solution must adequately describe the consequences to replay protection as a result of IPsec failover. For replay protection, it may be best for the replacement gateway to assume that the IPsec SA state is outdated and reestablish the IPsec SA using an IKEv2 CREATE_CHILD_SA exchange.

- IPsec failover facilitates the replacement of an IPsec GW serving a client with another GW. The design must take into account the possibility of an adversary creating a ping-ponging scenario where a client may be forced to move between two or more GWs persistently.

- It may be plausible for an attacker to force failover of a client to a gateway that is more advantageous to the attacker. The design must provide a means of verifying that a particular gateway belongs to the secure domain that the client may attach to using the same IKE SA.

8. IANA Considerations

No IANA action is required for this document.

9. Acknowledgments

We thank Russ Housley, Jun Wang, Marcello Lioy, and Raymond Hsu for technical discussions and/or help with standardization aspects related to this work. We thank Steve Kent for his review of the draft. We also thank Kuntal Chowdhury, Vijay Devarapalli and Kent Leung for their discussions on the applicability to Mobile IPv6 and 3G networks in general.

10. References

10.1. Normative References

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

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

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

[4] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

10.2. Informative References

[5] Wakikawa, R., "Home Agent Reliability Protocol", draft-ietf-mip6-hareliability-01 (work in progress), March 2007.

Author's Address

Vidya Narayanan (editor)
Qualcomm, Inc.
5775 Morehouse Dr
San Diego, CA
USA

Phone: +1 858-845-2483
Email: vidyan@qualcomm.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).