Abstract

Recovering from failure of IPsec gateways or servers 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 .................................................. 3
2. Introduction ................................................. 3
3. Terminology ................................................... 4
4. Applicability and Problem Statement ......................... 4
5. IPsec Failover Redundancy Solution Goals .................... 6
6. Security Considerations ....................................... 7
7. IANA Considerations .......................................... 8
8. Acknowledgments ............................................... 8
9. References ................................................... 8
   9.1. Normative References ..................................... 8
   9.2. Informative References .................................... 9
Author’s Address ................................................. 9
Intellectual Property and Copyright Statements .................. 10
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.

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 servers (for stateful operation) or on the client itself (for stateless
operation). Either the recovered IPsec entity or other entities in
the server pool may retrieve the stored IPsec and IKEv2 state for
faster recovery.

There are a number of proprietary solutions for 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 HA 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. 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) to lookup the relevant IPsec, encapsulates the
packets and sends to the appropriate VPN client.
IPsec 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 typically 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 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 cannot always be transparent to the client and hence, an interoperable protocol becomes very important.
5. 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.

- 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.

- Client Involvement: Given that the gateways may be distributed, the failover is not intended to be transparent to the client. The goal is to allow the client to initiate the switch to a different gateway.

- 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, the failover should not require EAP authentication, to avoid AAA overloading and possible user interaction.
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).

Interoperability: Client-gateway and gateway-gateway interoperability is required. This follows from the discussion on the other goals stated above.

Stateless Gateway Operation: The IPsec failover mechanism should specify a mode of operation that will allow the backup gateways to remain stateless until a failover occurs or during a temporary service interruption. 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.

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.

6. 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.

Solutions for a client-server model, where the client always initiates the secure communication may allow the client to find
the new server address through external means. Subsequently, the client must be able to verify the server’s authorization by verifying the proof of possession of the IKEv2 key material at the new server. A client should be able to initiate a new IKEv2 SA with one or more auxiliary servers without interrupting a connection to the currently used primary server. The client must consider the new server as a provisional server until it has verified a new server is the appropriate replacement for the primary server.

- 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 server to assume that the IPsec SA state is outdated and reestablish the IPsec SA using an IKEv2 CREATE_CHILD_SA exchange. (Perhaps this can be relaxed after a more in-depth analysis).

- 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.

7. IANA Considerations

No IANA action is required for this document.

8. Acknowledgments

We thank Russ Housley, Jun Wang, Marcelllo Lioy, and Raymond Hsu for technical discussions and/or help with standardization aspects related to this work.

9. References

9.1. Normative References


9.2. Informative References

draft-ietf-mip6-hareliability-00 (work in progress), June 2006.

Author’s Address

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

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