IPsec Failover and Redundancy Problem Statement and Goals

draft-vidya-ipsec-failover-ps-01

Presented by: Yaron Sheffer

Contributors

- Lakshminath Dondeti
- Paul Hoffman
- Tero Kivinen
- Gregory Lebovitz
- Marcus Leech
- Cheryl Madson
- Vidya Narayanan (Ed.)
- Michael Richardson
- Sheela Rowles
- Yaron Sheffer
- Marcus Stenberg
- Brian Weis

The Problem

- **Fast re-establishment of IPsec SAs**
- **What forces clients to re-establish IPsec SAs**
  - Network failures (affect reachability to IPsec gateways)
  - Gateway failures
  - Failure of application servers using IPsec
- **Issues with re-establishment**
  - Large number of clients establishing SAs with gateways after failover in a short time span
    - **IKEv2 is computationally expensive**
      - **DH and potential use of public keys**
    - **When EAP is used for client authentication in IKEv2**
      - **SA establishment involves several more roundtrips**
      - **User may be prompted again for credentials**
      - **Too many hits on the AAA server**

Applicability

- **Servers using IPsec**
  - Other applications such as Mobile IPv6 use IPsec for protection of signaling
    - **IPsec may be used in tunnel or transport mode**
  - Applications may have interoperable solutions for server failover
    - **Incomplete without IPsec failover**
    - **Either interoperability or seamless failover is not available without IPsec failover**
  - Application servers handling large number of clients have to handle large number of IPsec SAs
    - **SAs may be a mix of transport and tunnel mode**
- **IPsec Gateways**
  - Always handle tunnel mode traffic

IPsec Failover Solutions Today

- **Run IKEv2 again with the new gateway**
  - Inevitable today when the gateway address changes
  - Inevitable if client or gateway has reset the session state
- **Proprietary solutions exist when gateways have the same address**
  - Failover transparent to clients
  - Gateway to gateway SA transfer protocol is proprietary
- **What's wrong with this state of affairs?**
  - Problems with running IKEv2 again covered in the previous slide
  - Proprietary solutions have obvious limitations
    - **Gateways cannot be distributed globally without complex network planning**
    - **Gateways cannot all be active for the same IP address**
    - **Lack of interoperability**

Solution Goals (1/2)

- **Distributed Failover**
  - Gateways may be located at different sites and may not share the same IP address or have the same view of the network
- **Client Involvement**
  - Given that the gateways may be distributed, the failover cannot be transparent to the client
- **Low Latency failover**
  - IPsec gateway having to handle a flood of IKEv2 exchanges upon a failover
  - Low latency requirements of applications that use IPsec, e.g., Mobile IPv6
- **Application Usage of IPsec**
  - Need to take requirements of applications of IPsec in designing the failover solution

Solution Goals (2/2)

- **Interoperability**
  - Client-gateway and gateway-gateway interoperability is required
- **Stateless Failover**
  - Infrastructure remains stateless; state is stored in the client
- **Stateful Failover**
  - Must be possible to store IKEv2/IPsec state in the infrastructure
- **Support for IPsec transport and tunnel modes**

Thank You!