IKEv2 Security Gateway Discovery

draft-mglt-ipsecme-security-gateway-discovery-00.txt

D. Migault, K. Pentikousis

12/03/2013- IETF86- Orlando

Addressed Problem

This draft considers the following situation:

- A VPN Client is attached to a Security Gateway (IKEv2 + VPN)
- The VPN service is provided by a distributed VPN platform
- The VPN Client is likely to change the SG it is attached to
  - Because of VPN Client mobility and change its point of attachement
  - Because other Security Gateway may provide better connectivity
  - ...

The problem addressed is: How can the VPN Client chose the best Security Gateway

- A VPN Client to request information on neighboring SGs
- A Security Gateway to provide information on neighboring SGs

Use cases

ISPs offloading RAN traffic to Security Gateway located in DSL Boxes

- Mobile VPN Client wants to move from one SG to the other
- Next SG MUST be appropriately selected,
- VPN Clients may prefer a SG with VPN mobility (intra-SG communication)

The VPN service is provided by a large distributed / cluster of VPN

- All SGs of the cluster may not provide the same QoS (congestion, load...)
- Next SG may be more available, with better bandwidth
- VPN Clients may prefer a SG with VPN mobility (intra-SG communication)
- VPN Clients with MOBIKE may perform traffic management and prefer:
  - SG with multiple interfaces on multiple networks
  - Change their interface if they have multiple interfaces

Security Gateway Discovery Protocol

The SGDP mainly consists of a Query / Response exchange with:

- A NEIGHBOR_INFORMATION Notify Payload with a Query/Response bit
- A response embeds a list of NEIGHBOR attribute
- Each NEIGHBOR is associated with some Neighbor Options

The different attributes we considered are:

- O-REQUEST: Option (information) requested for each NEIGHBOR
- PADDING: to align with 32 bytes Notify Payloads
- NEIGHBOR: a neighboring Security Gateway
- MAX-NEIGHBOR: to limite the size of responses

Security Gateway Discovery Protocol

Neighbor Options for NEIGHBOR attribute we are considering:

- _INTERFACE: list of IP addresses
- _GEOLOC: Geolocalisation
- _ISG-BW: Intra Security Gateway bandwidth
- _ISG-MOB: Intra Security Gateway mobility mechanisms