Encapsulating IPsec ESP in UDP for Load-balancing draft-xu-ipsecme-esp-in-udp-lb-15

Xiaohu Xu@China Mobile
Shraddha Hegde@HPE
Boris Pismenny@Nvidia
Dacheng Zhang@Huawei
Liang Xia@Huawei
Mahendra Puttaswamy@HPE

IETF125, Shenzhen

Motivations

- IPsec VPNs are widely used by enterprises to connect geographically dispersed branch offices over the Internet. They are also increasingly employed by cloud providers to encrypt DCI WAN traffic, helping meet security and compliance requirements.
- To fully utilize available WAN or Internet bandwidth, effective load balancing of IPsec traffic across ECMP and/or LAG is essential. While some cloud providers support multiple parallel IPsec tunnels for ECMP, this approach is far from ideal.
- Encapsulating IPsec ESP packets over UDP tunnels with the UDP source port being used as an entropy field will enable existing data center switches and core routers to perform efficient load-balancing of the IPsec ESP traffic without requiring any change to them.

Motivations (con't)

- IPsec VPN gateways are usually implemented in the form of multi-core x86 servers. Receive Side Scaling (RSS) is a widely adopted network driver technology which spreads incoming TCP or UDP traffic across multiple CPUs by performing hash function on the network and/or transport layer headers, resulting in increased multi-core efficiency and processor cache utilization.
- Encapsulating ESP in UDP would facilitate RSS to distribute the received IPsec traffic more evenly across multiple CPU cores.

Solution Overview

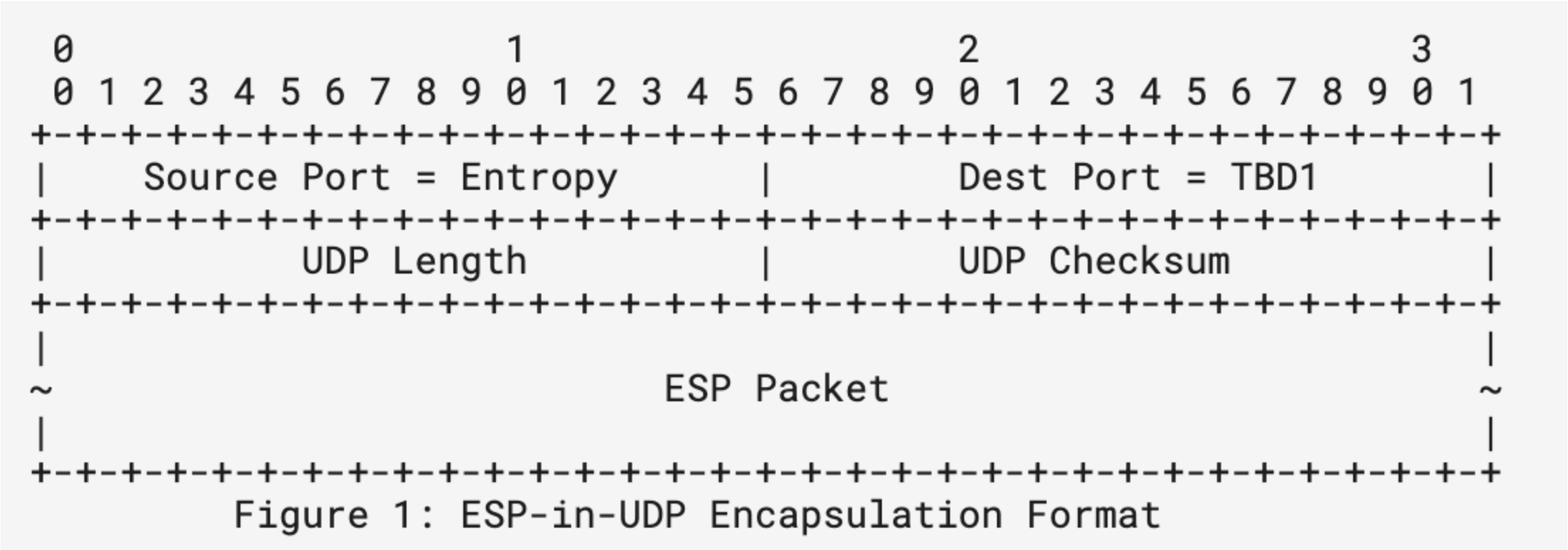

Figure 1: ESP-in-UDP Encapsulation Format

- Source port field contains a 16-bit entropy value that is generated by the encapsulator to uniquely identify a flow.

Implementation Status

- It has been implemented by some network vendors. One example is Juniper Networks/HPE (https://www.juniper.net/documentation/us/en/software/junos/interfaces-adaptive-services/topics/topic-map/ipsec-overview.html).

Next Step

- The document is ready for the WG adoption call.