Multi-Segments SD-WAN via Cloud DCs
draft-ietf-rtgwg-multisegment-sdwan-02

Kausik Majumdar ([Argus Networks](mailto:Argus%20Networks))
Linda Dunbar ([ldunbar@futurewei.com](mailto:ldunbar@futurewei.com))
Venkit Kasiviswanathan ([venkit@arista.com](mailto:venkit@arista.com))
Ashok Ramchandra ([aramchandra@microsoft.com](mailto:aramchandra@microsoft.com))
Aseem Choudhary ([achoudhary@aviatrix.com](mailto:achoudhary@aviatrix.com))

IETF 120 July 2024, Vancouver
Geographic Faraway Branches Connected via Cloud Backbone

Why?

- The public internet among those branches might have limited bandwidth, unpredictable connection, or be prone to cyber-attacks.
- The network paths from CPEs to the Cloud GW have more reliable connections and are constantly monitored by sophisticated network functions.
- Easier to utilize Cloud-based security functions, such as Firewalls, DDoS, etc., to apply consistent policy enforcement for workloads/services to the Cloud and across the branches.
- Easier to utilize the Cloud-based tools and SaaS to collect and analyze the threat of traffic.
- Utilize the Cloud Backbone to interconnect those branches.
Steering Encrypted Flows through Backbone Network

Environment:
- “a” (CPE) has IPsec SAs to GW1/GW2 for connecting to services hosted in the Cloud.
- “b” (CPE) has IPsec SAs to GW10/GW20 for connecting to services hosted in the Cloud.

Goal:
- steer the IPsec encrypted flows from “a” to “b” through GW2→P20→GW10, using encapsulation header (e.g., GENEVE)

IPsec ESP encrypted flow from “a” to “b”
Major Components

- GENEVE Multi-Segment SD-WAN Option Class
- SD-WAN Tunnel Endpoint Sub-TLV
- SD-WAN Tunnel Originator Sub-TLV
- Egress GW Sub-TLV
- Include Transit Sub-TLV
- Exclude Transit Sub-TLV
- HMAC-Auth-Val Sub-TLV
Major Changes

- GENEVE Option Class value (x0163) has been assigned to Multi-segment SD-WAN
- Added the description of all the fields in the SubTLVs.
- Revised the illustration of packet format from CPEs to Cloud GW, through Cloud Backbone, and to destination CPEs.
- Moved the illustration to Appendix
Next Step:

• Need GENEVE experts to provide technical review
• Work with authors for draft-boutros-nvo3-ipsec-over-geneve
• Need more reviewers