Multi-Segments SD-WAN via Cloud DCs

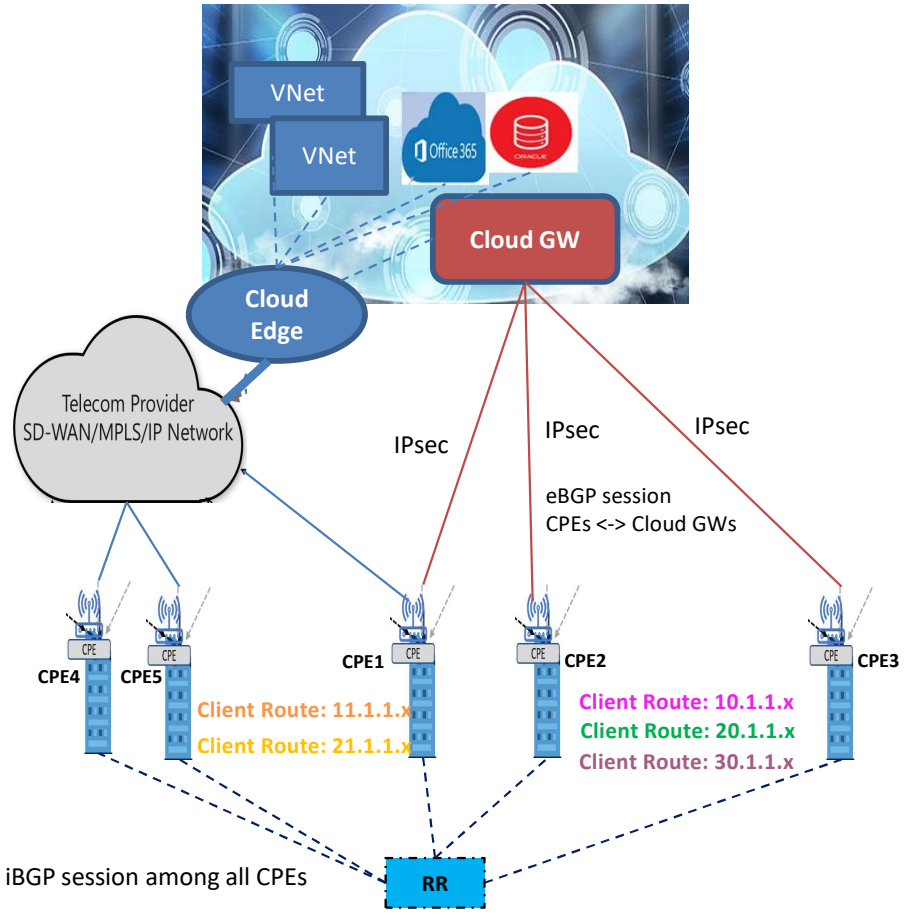
draft-dmk-rtgwg-multisegment-sdwan-04

Kausik Majumdar(kmajumdar@microsoft.com)
Linda Dunbar (ldunbar@futurewei.com)
Venkit Kasiviswanathan (venkit@arista.com)
Ashok Ramchandra (aramchandra@microsoft.com)
Aseem Choudhary (achoudhary@aviatrix.com)

IETF 118 Nov 2023, Prague

Background: Multi-Segment SD-WAN Scenario 1:

via Single Transit GW within a Cloud DC
without the Cloud GW terminating IPSec Tunnels.

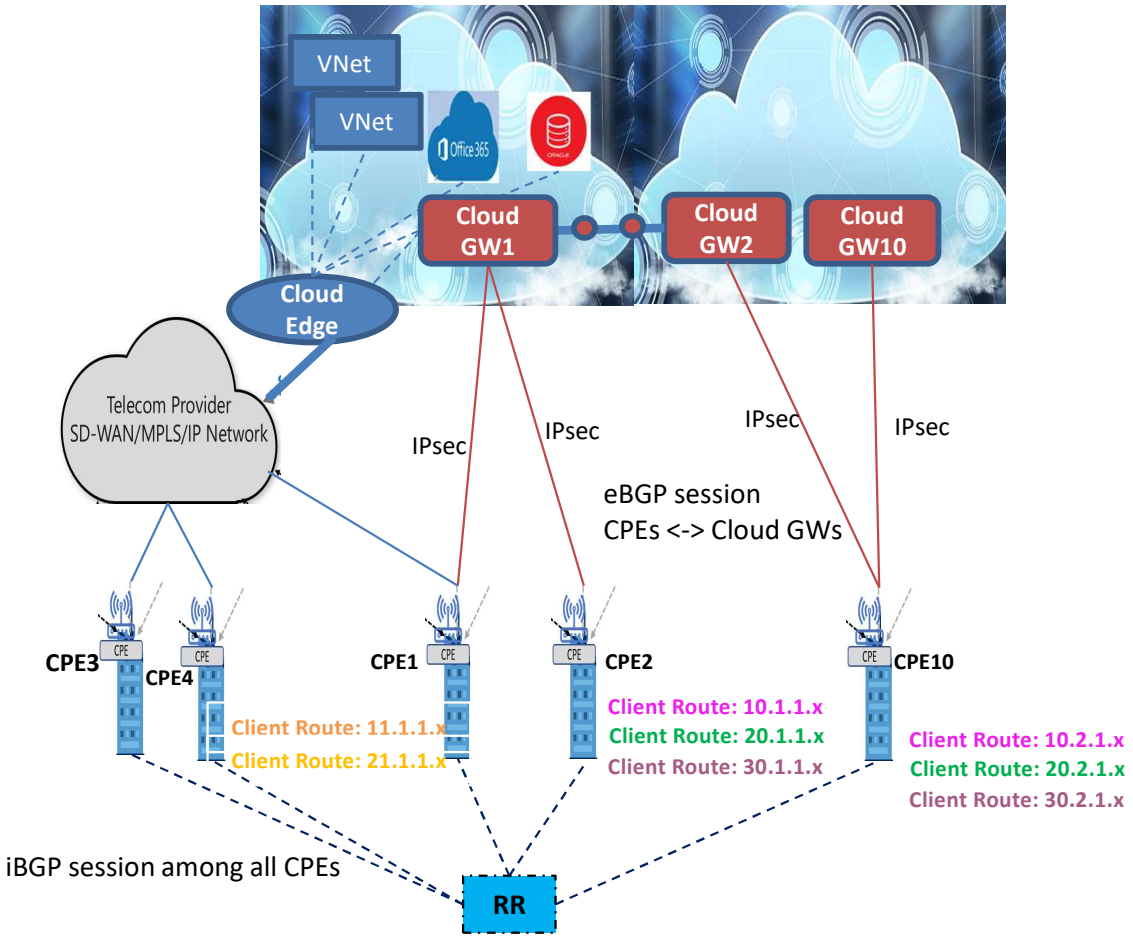


Benefits:

- 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.

Multi-Segment SD-WAN Scenario 2:

Branch <-> Branch traffic via Cloud Backbone



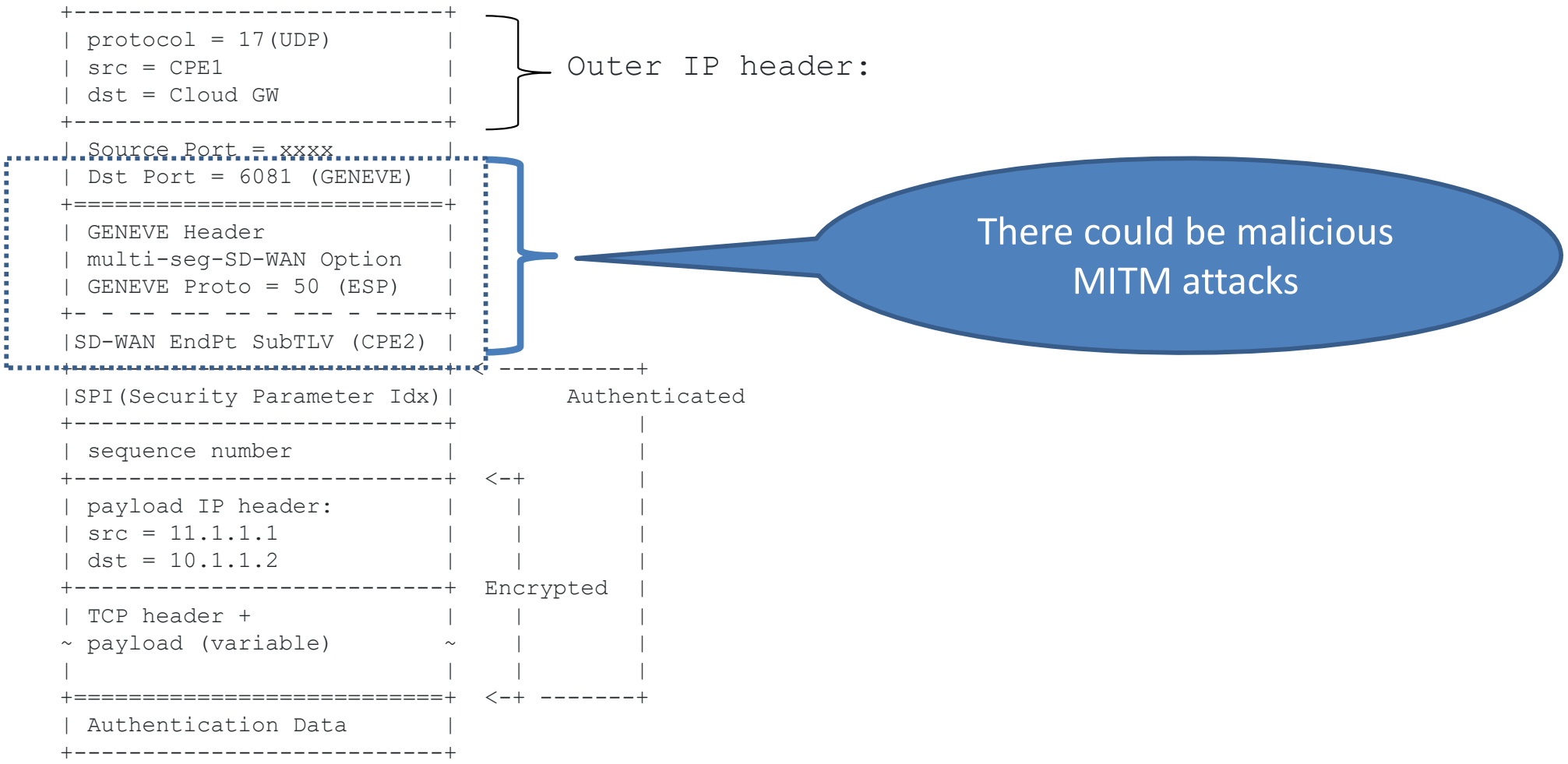
Multiple Cloud GWs in Different Regions.

The geographic faraway branches can establish SD-WAN paths to their corresponding Cloud GWs to access Cloud services in different locations.

Benefit:

- Utilize the Cloud Backbone to interconnect those branches.
- Plus, All the benefits of single Cloud GW.

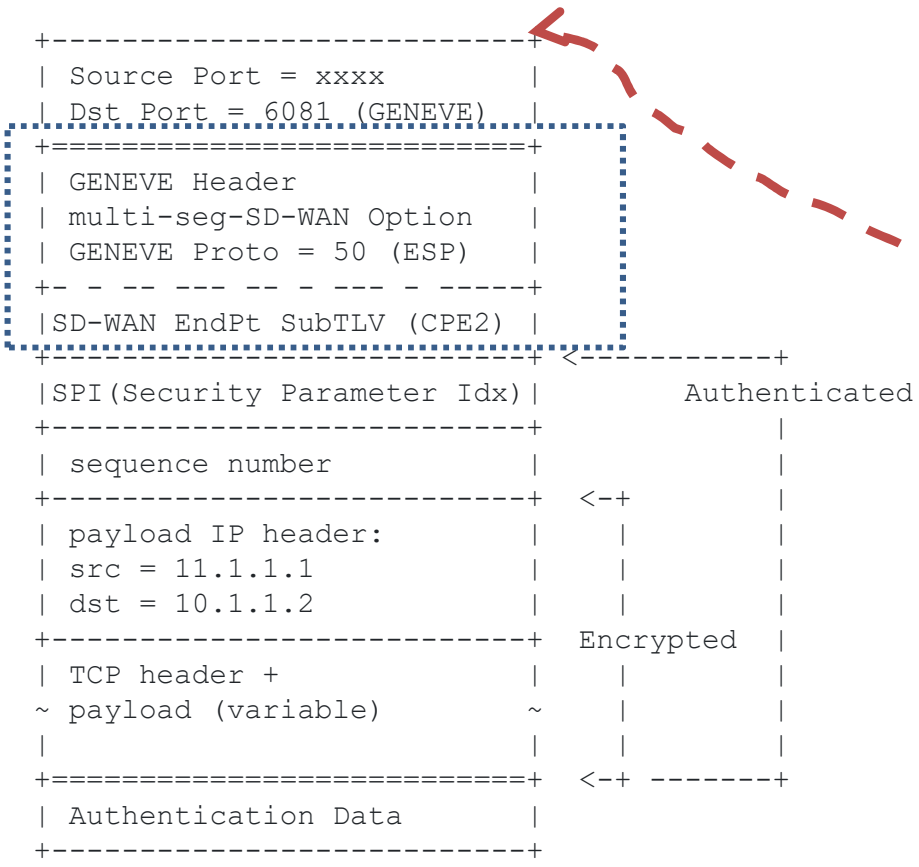
-03 Major Addition: Security Considerations

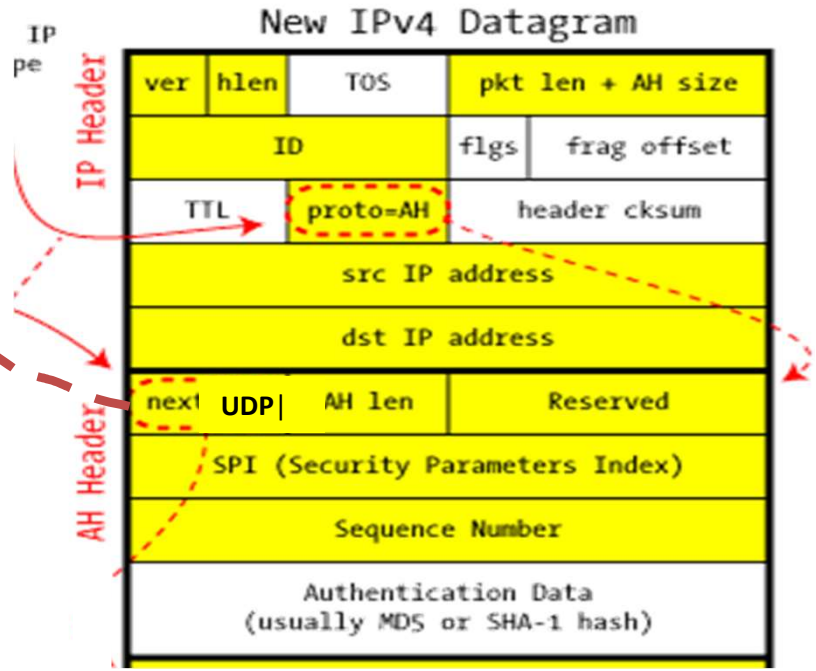


Threat Analysis

- **Added to the Security Consideration Section**
  - Eavesdropping:
    - no different from direct IPsec SAs between two CPEs.
  - Data Manipulation:
    - unrecognized source addresses or invalid values in the Sub-TLVs of the GENEVE header are dropped by Cloud GWs, there might be a higher packet drop rate between the CPEs.
  - Potential steeling of Cloud Backbone bandwidth:
    - Mitigation method: data integrity and authentication for traffic between CPEs and Cloud GWs

To Mitigate MITM Attacks: Add AH Header to Authenticate





Problem: Can't traverse NAT because the outer IP address changes.

Simpler Method: Do Nothing

- Both AH & ESP-NULL require pairwise key management between CPE & Cloud GW.
- Since the data between CPEs are encrypted, the consequence of MITM attacks is packets being redirected to the wrong destinations resulting in packets dropping.
  - Each deployment can weigh the cost and consequences to make the appropriate choice.

Enhanced Authentication and Integrity Check

- Section 9.2 (New) : HMAC-based Integrity and Authentication
  - The IPsec SA already encrypts the client payload between the CPEs, the Cloud GW doesn't need to decrypt and re-encrypt the payload when relaying it to the destination CPE.
  - HMAC (Hash-Based Message Authentication Code) can be used to ensure the integrity and authenticity

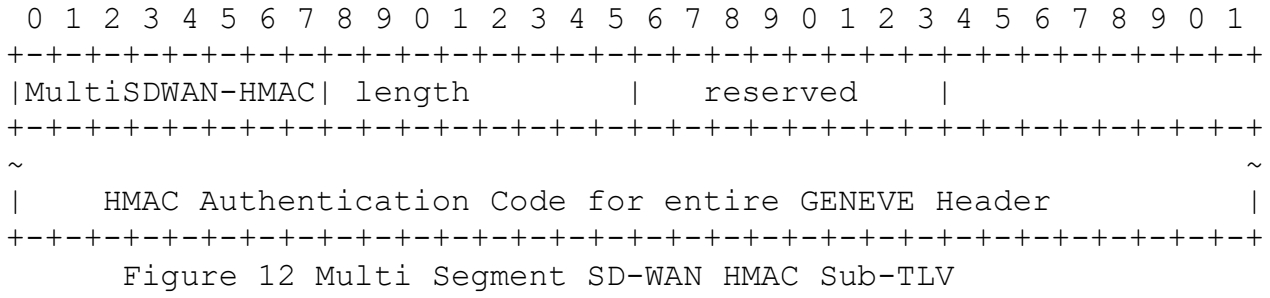


Figure 12 Multi Segment SD-WAN HMAC Sub-TLV

The HMAC Authentication Code, a.k.a. the HMAC hash value, is computed including all the bytes in the GENEVE header and with the MultiSDWAN-HMAC value field setting to 0.

Feedback from SEC area experts:

- Russ Housley: HMAC with SHA-256 seems like a fine choice.
- Darren Dukes:
  - Improvement on the analysis of pros & cons of using HMAC

Next Step: Looking for Feedback/Comments

- Asking for WG Adoption.