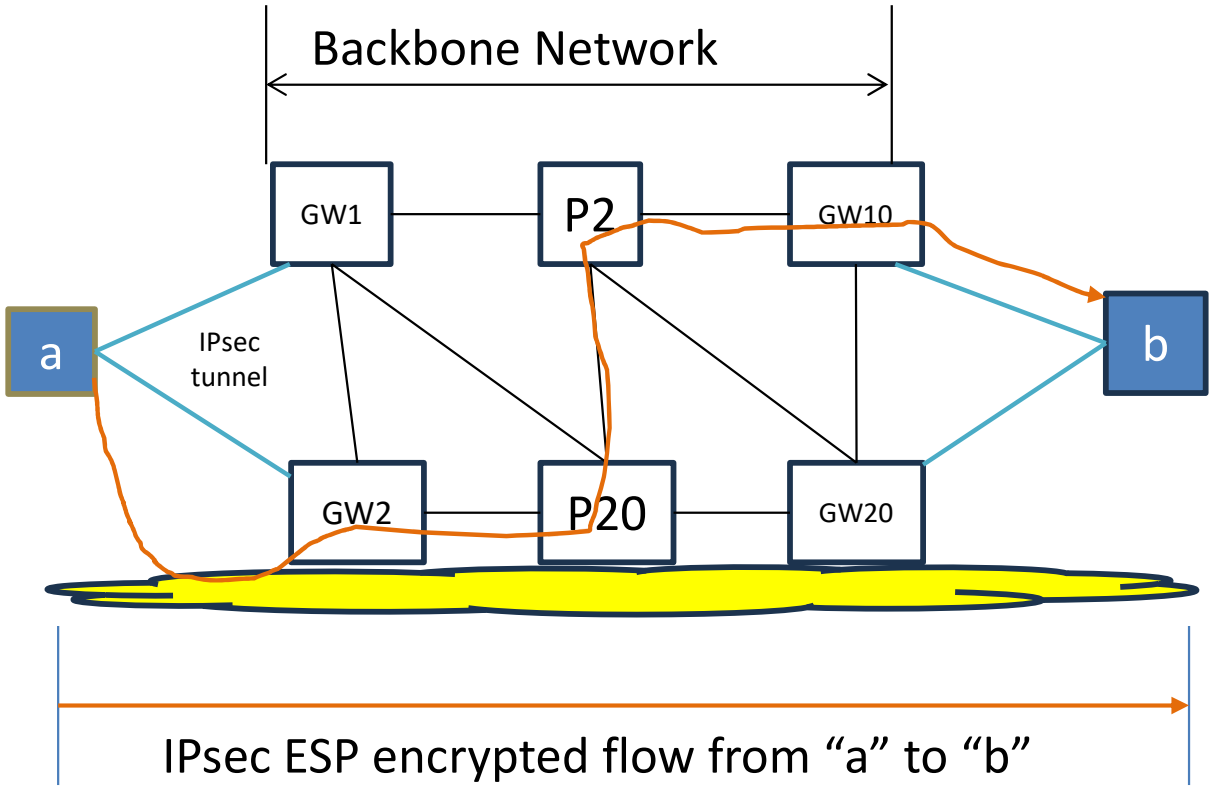
Lightweight Authentication Methods for IP Encapsulation Header

draft-dunbar-secdispatch-ligthtweight-authenticate-03

Linda.Dunbar@Futurewei.com
Kausik.Majumdar@Oracle.com
Scott.Fluhrer@Cisco.com

IETF 121 Nov 2024, Dublin

Steering Encrypted Flows through Backbone Network

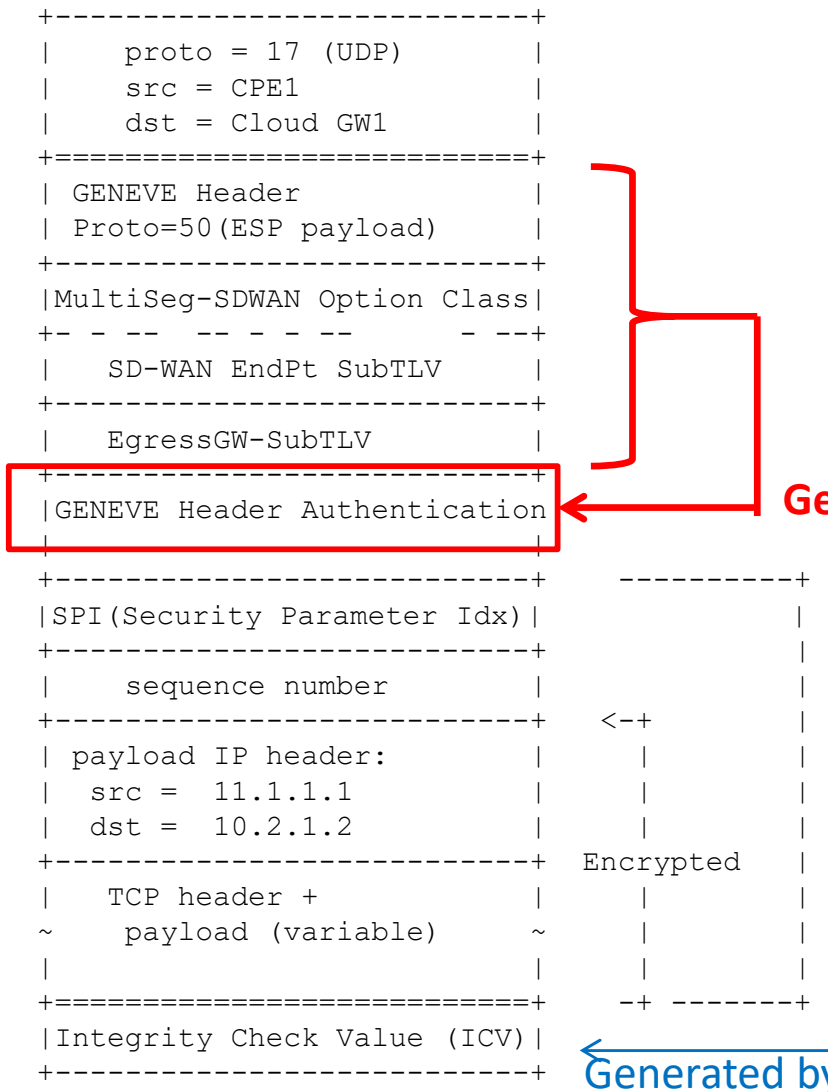


Goal:

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

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.



Selective Authentication:

- GWs selectively validate the GENEVE Header Authentication code, based on pre-configured policy
- Pre-configured policy: some flows don't need authenticating the GENEVE header, yet a dummy value is included in the packet.

Generated by "a", validated by "GW2"

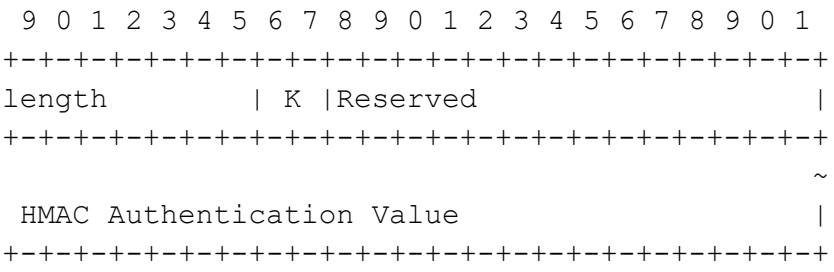
Why?

- ❑ "GW1, 2, 10, 20" have limited capacity in processing IPsec. For IPsec encrypted flow from "a" to "b", GW doesn't need to decrypt the flow.
- ❑ Useful in environments where the computational cost of authenticating every packet header is prohibitively high

Generated by "a", validated by "b"

Key Management

- **Key Generation:** The backbone network controller is responsible for generating a set of **symmetric keys**. These keys are specific to each SD-WAN session and are securely distributed to edge devices.
- **Key Storage:** Edge devices are responsible for securely storing the keys
- **Key Rotation:** edge devices initiate key rotation. The new index is indicated in the Auth-Val field:



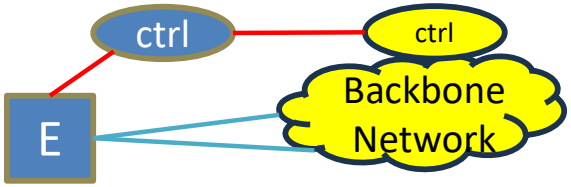
K Flag (2 bits): indicates the index of the key used for computing the HMAC Authentication Value present in the TLV.

- **Key Revocation:** The backbone controller is responsible for revoking keys; when timer is expired or key compromise is detected.

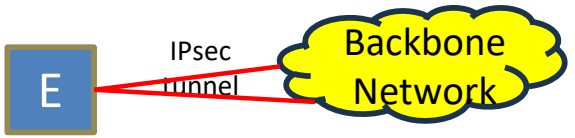
Key Distribution

- **Initial Distribution:** Keys are distributed to edge devices at the start of each SD-WAN session.
- **Key Updates:** SD-WAN session is restarted when new set of keys are distributed

- **Via Secure Control Plane**
  - assumes the presence of a secure channel between the two organizations for key exchange. It also assumes a secure channel exists between the network controller and the CPEs.



- **Via Secure Data Plane Tunnel**
  - IPsec tunnel provides a secure channel for transmitting authentication keys



- existing IPsec keys can be used as input to a key derivation function (KDF)
  - The KDF generates unique authentication keys that are cryptographically linked to the IPsec keys

Control Plane

- The configuration for the frequency and selection of flows that undergo real authentication
- When a network segment is detected to have a higher than usual probability of security risks, several actions can be taken:
  - Increase the frequency of flows to be fully authenticated
  - Move towards comprehensive authentication where all packet headers are authenticated, rather than just selective flows
  - Adding another layer of encryption for the header between CPEs and Cloud GWs

Looking for Feedback/Comments