

Lightweight Authentication Methods for IP Encapsulation Header

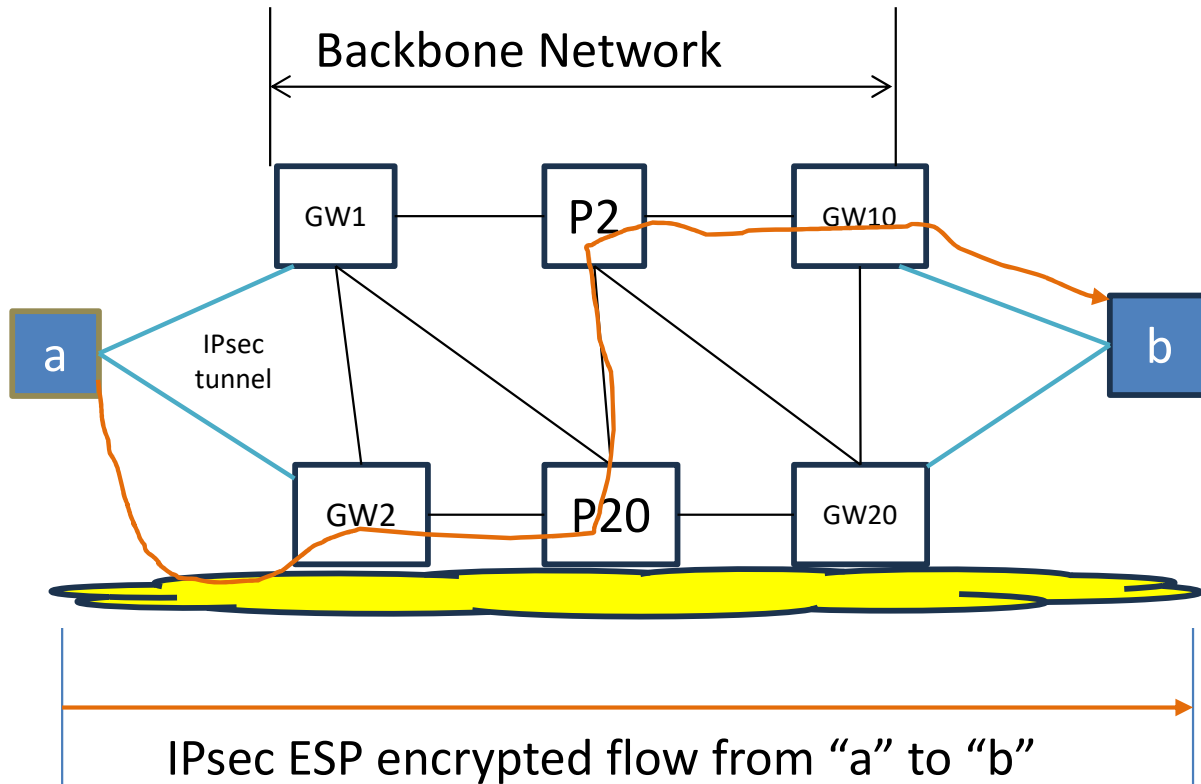
draft-dunbar-secdispatch-lightweight-authenticate-02

Linda Dunbar ([Futurewei](#))

Kausik Majumdar([Argus Networks](#))

IETF 120 July 2024, Vancouver

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.

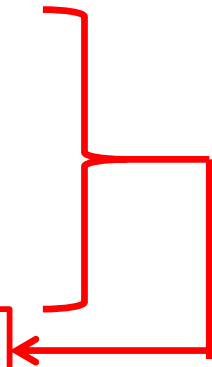
```

+-----+
| proto = 17 (UDP) |
| src = CPE1 |
| dst = Cloud GW1 |
+=====+
| GENEVE Header |
| Proto=50 (ESP payload) |
+-----+
| MultiSeg-SDWAN Option Class |
+-----+
| SD-WAN EndPt SubTLV |
+-----+
| EgressGW-SubTLV |
+-----+
| GENEVE Header Authentication |
+-----+
| SPI (Security Parameter Idx) |
+-----+
| sequence number |
+-----+
| payload IP header: |
| src = 11.1.1.1 |
| dst = 10.2.1.2 |
+-----+
| TCP header + |
| ~ payload (variable) ~ |
+-----+
| Integrity Check Value (ICV) |
+-----+

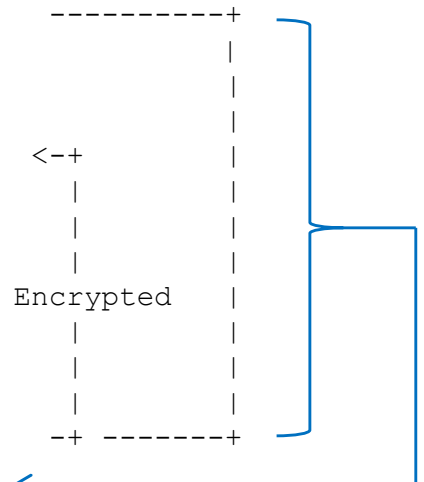
```

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"



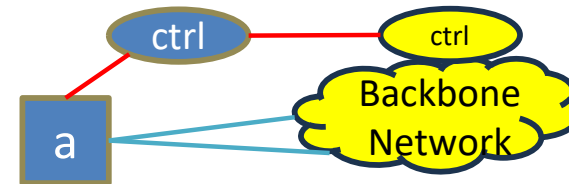
Generated by "a", validated by "b"

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

Authentication Key Distribution

- 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