Geneve Security Requirements

Migault - Boutros - Wing - Krishnan

Discussions: transit nodes

The current draft considered that transit nodes are on path Geneve tunnels and are able to process Geneve options.

Discussions considered that transit nodes as being part of the NVE which makes Geneve option processing by on-path transit nodes out of scope.

- This should be clarified in the architecture document and out of scope of the requirement draft.
- Next version will consider transit nodes integrated to NVE.
- However, this aspect has numerous security implications.
  - NVE-NVE security versus multiple hop security
  - Are Geneve option mutable immutable ?

Discussions: security model

The draft considered 3 layers that should be able to secure their layer independently.

- Cloud providers
- Geneve Overlay Network administrator
- Tenants

Discussions are on having the Cloud Provider as the Geneve Overlay Network administrator.

- No much implication without transit nodes

Discussions scope

The initial scope of the document was to set the requirement for a Geneve Security option or a mechanisms for an overlay network to secure the Geneve overlay

The document has been extended to include requirements so Geneve deployment reliably secure the transit of Tenants traffic.

Discussions are whether such Geneve Security option is is necessary, and whether everything should not be provided by NVE-NVE communication encryption.

Security optimization versus requirements

DTLS provides Encryption + Authentication + antireplay of the WHOLE packet.

- Tenant using IPsec/TLS already encrypt their payload
  - Double encryption: Using DTLS may be overkill
- Authentication of the Geneve Header
  - Encrypting the whole packet with DTLS may be overkill
- Multicast
  - Does not work with DTLS
  - IPsec

Discussion are around whether only IPsec/DTLS should be considered.

Flows Management

Should we be able to have multiple flow with different level of security within a Geneve Tunnel ?

Thanks!