Geneve Security Requirements

Migault, Boutros, Wing, Krishnan

Purpose of the document

Requirements may have multiple purposes:

1. Listing all possible security requirements in order to define a Generic Security Mechanisms for Geneve.
    a. Generic does not mean necessarily new, but it means it can be applied in every case
2. Listing the a comprehensive list of security requirements that enable a network administrator to determine if its deployment of Geneve is secured.
    a. Deployment specific security mechanism may be based on assumptions, re-use a given technology already in place…. But provide the expected security.
    b. Typically using DTLS / IPsec between NVE is likely to secure the Geneve overlay for 90 % of the deployment but is limitative for the remaining 10 %.

Purpose of the document

The current document addresses 1, but partrly not 2.

Requirements are listed given the threat to mitigate.

- Leave the specific deployment to define which requirements applies given the threats he wants to mitigate (Policies) .

Requirements may also depends on additional policies (e.g per-flow policies), deployment considered (e.g the presence or not of GTN), the usage of options....

- This needs to be specified so a network architecture get the requirements that applies to its current setting.

Purpose of the document

We will re-organize the document providing for each Requirement the context it applies or not.

`Conditions:`

- `Requirement A`
- `...`
- `Requirements N`

The message over all is that most deployments can already secure their Geneve overlay without the design of a Generic Geneve Security Mechanism.

Inconsistencies with draft-ietf-nvo3-security-req.

With the given structure `( Condition, Requirements )` versus `( Requirements )` may end in apparent inconsistencies:

- `Condition` is implicitly mentioned with a MAY
- Explicit `Condition` may result in MUST / SHOULD

This will result in only an apparent inconsistencies, but currently we did not notice inconsistencies between the drafts.

Position with draft-ietf-nvo3-security-req.

Geneve is a subset of NVO3 and NVO3 security requirements should not be repeated in Geneve security requirements.

Given the status of draft-ietf-nvo3-security-req we would like guidances on:

- Providing a self contained document
- Avoiding overlaps between the two documents.

Thanks!