Geneve Security Architecture

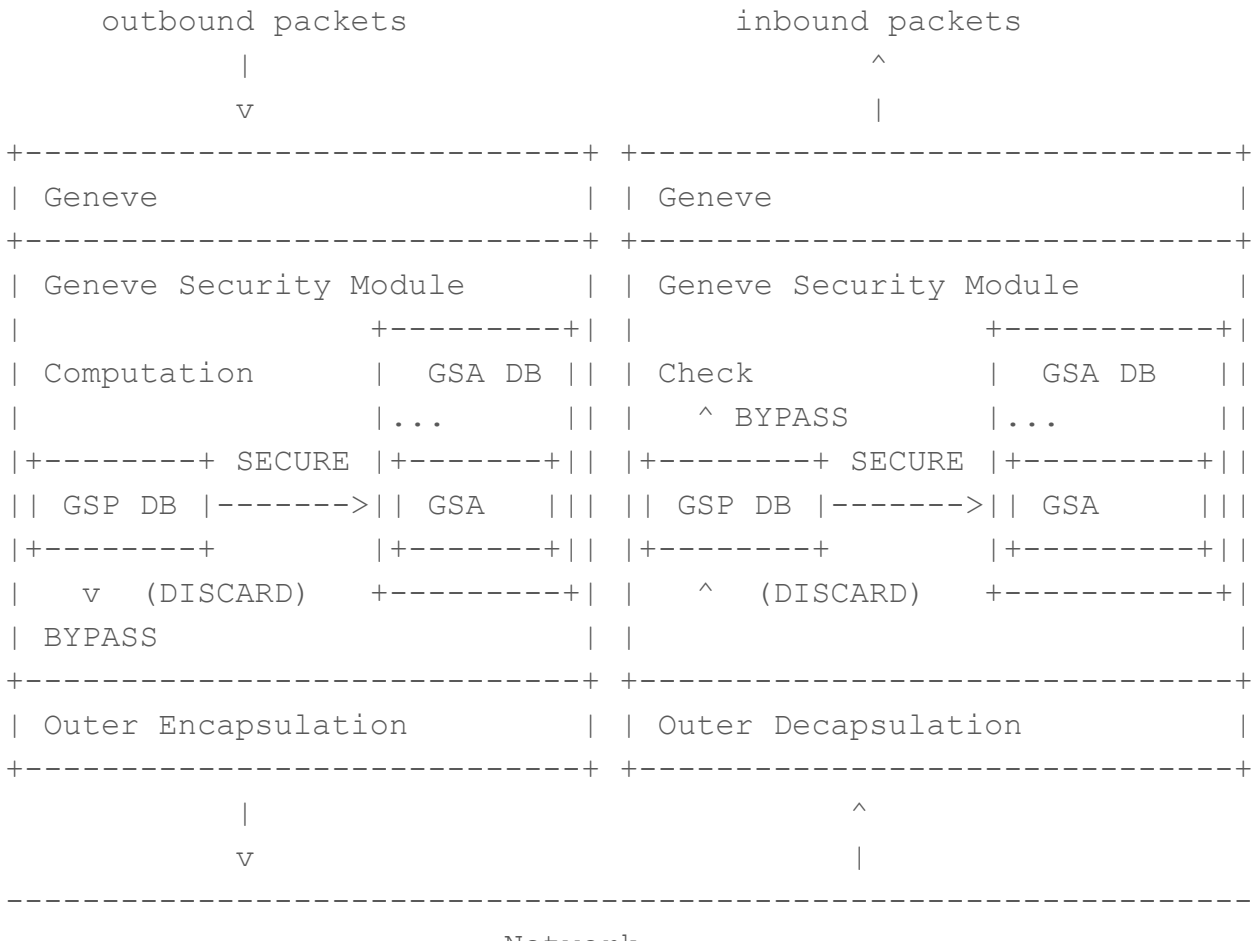
draft-mglt-nvo3-geneve-security-architecture-00

Migault IETF99

Security Architecture

The primary goal of the security architecture is to coordinate the security policies associated to the different flows:

- Associate a security policy to a given flow
- Derive the appropriate transformations from the policies
- Check that received packets match the security policy
  - Your packet might be authenticate by you expected it to be encrypted.
  - A packet may be decrypted correctly, but the decrypted packet may be associated a DISCARD security policy


outbound packets
inbound packets
Geneve
Geneve Security Module
Computation
GSA DB
SECURE
GSP DB
GSA
(DISCARD)
BYPASS
Outer Encapsulation
Geneve
Geneve Security Module
Check
GSA DB
BYPASS
SECURE
GSP DB
GSA
(DISCARD)
Outer Decapsulation
Network

Geneve Security Architecture

Follows the principles of the IPsec security architecture:

- Geneve Security Policies (GSP): Defines which Geneve Packet is associated to DISCARD, BYPASS or SECURE.
  - Determination of the Geneve Packet is done through Traffic Selector
- Geneve Security Association (GSA) contains the cryptographic material necessary to process a Geneve Packet associated with a SECURE GSP.

Traffic Selector: Which are the necessary selector ?

Fields of the Geneve Fix Header:

- Geneve Version ?
- OAM bit
- Critical bit
- Rsv
- Protocol Type
- VNI

Traffic Selector: Which are the necessary selector ?

Additional Selectors:

- Next Header (IPv6) / Protocol (IPv4) (8 bits): to track IPsec/ESP, IPsec/AH, TCP, UDP…
- Ports: to track (D)TLS or unprotected services HTTPS, HTTP…
- Traffic selector should also include non-IP protocols (IPX, Appletalk, DECnet, whatever you like), and also non-UDP/non-TCP (e.g., RSVP, GRE, DCCP, SCTP).

This is only useful if we have different treatment for these flows.

Outbound Processing

The Geneve Security Module consults the GSP DB to determine the GSP associated to the Geneve Packet.

- DISCARD
- BYPASS
- SECURE: one or multiple Geneve Security Associations (GAS) are returned

The Geneve Security Module process the GAS (GAO/GEO)

Inbound Processing

The Geneve Security Module checks the Geneve Packet is associated to a DISCARD or a BYPASS or SECURE

The Geneve Security Module opens a security context which lists the encountered and validated GSO as well as their respective order. For each GSO:

- extract the GSA-ID of the GSO
- Retrieve the corresponding GSA (if not found goes to the next GSO)
- Validation of the GSO against the GSA (including Selectors).

The Geneve Packet is matched against the GSP DB to validate the GSA-ID listed in the security context match those returned by the GSP DB.

Thanks!