

NV03  
Internet-Draft  
Intended status: Standards Track  
Expires: December 29, 2017

D. Migault  
June 27, 2017

Geneve Security Architecture  
draft-mglt-nvo3-geneve-security-architecture-00

## Abstract

This document describes the Geneve Security Architecture.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 29, 2017.

## Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

Geneve Security Architecture

June 2017

## Table of Contents

<a href="#">1.</a>	Requirements notation . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">3.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Architecture Overview . . . . .	<a href="#">4</a>
<a href="#">5.</a>	Geneve Security Policies Database . . . . .	<a href="#">5</a>
<a href="#">5.1.</a>	Selectors . . . . .	<a href="#">6</a>
<a href="#">5.2.</a>	Geneve Security Policies . . . . .	<a href="#">8</a>
<a href="#">5.3.</a>	Geneve Security Policies Example . . . . .	<a href="#">8</a>
<a href="#">6.</a>	Geneve Security Association Database . . . . .	<a href="#">11</a>
<a href="#">6.1.</a>	Geneve Security Associations . . . . .	<a href="#">11</a>
<a href="#">7.</a>	Geneve Security Module Packet Processing . . . . .	<a href="#">13</a>
<a href="#">7.1.</a>	Outbound Geneve Processing . . . . .	<a href="#">13</a>
<a href="#">7.2.</a>	Inbound Geneve Packet Processing . . . . .	<a href="#">13</a>
<a href="#">8.</a>	IANA Considerations . . . . .	<a href="#">14</a>
<a href="#">9.</a>	Security Considerations . . . . .	<a href="#">14</a>
<a href="#">10.</a>	Acknowledgment . . . . .	<a href="#">14</a>
<a href="#">11.</a>	References . . . . .	<a href="#">15</a>
<a href="#">11.1.</a>	Normative References . . . . .	<a href="#">15</a>
<a href="#">11.2.</a>	Informational References . . . . .	<a href="#">15</a>
	Author's Address . . . . .	<a href="#">16</a>

[1.](#) Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

[2.](#) Introduction

[I-D.ietf-nvo3-encap] and [[I-D.mglt-nvo3-security-requirements](#)] clearly state the need to secure the Geneve overlay network and provide means to authenticate the Geneve Header as well as being able to encrypt the Geneve Payload.

Both of these requirements are fulfilled with specific Geneve Security Options. More explicitly, [[I-D.mglt-nvo3-geneve-authentication-option](#)] defines an option that authenticate the Geneve fixed Header and optionally a set of Geneve Option as well as a portion of the Geneve Payload. [[I-D.mglt-nvo3-geneve-encryption-option](#)] defines a Geneve Option that enables to encrypt a subset of Geneve Options as well as a portion of

the Geneve Payload. Further descriptions on how an Geneve Security Option is treated is out of the scope of this document.

This document defines how the Geneve overlay can be secured properly. A Geneve Element may handle different Geneve overlay networks

associated with different level of security. This document defines how to associate a level of security to an Geneve overlay network. In addition, a security level for a given overlay network may result in a combination of multiple Geneve Security Options. As the order these Geneve Security Options are processed matters, it is necessary the sending and receiving Geneve Element have similar behaviours in order to guarantee interoperability while securing a Geneve overlay Network.

This document explains how Geneve Security Policies and Geneve Security Associations are organized to associate a given level of security to an Geneve overlay network. In addition, this document also exposes how the Geneve Security Module implementing the security interacts with the Geneve architecture.

### [3.](#) Terminology

- o Geneve Elements: designates all elements that handled Geneve Packets. These elements may be terminal elements such as NVEs for example, but can also be on path elements that are expected to manage the flow inside the Geneve overlay network.
- o Geneve Packet: designates the packet that Geneve Elements are expected to handled. It is composed of a Geneve Header and a Geneve Payload. In this document the Outer Ethernet Header and Outer IPv4 Header as well as the Outer UDP Header defined in [\[I-D.ietf-nvo3-geneve\] section 3.1](#) are not part of the Geneve Packet. Similarly, the Outer Ethernet Header, the Outer IPv6 Header as well as the Outer UDP Header defined in [\[I-D.ietf-nvo3-geneve\] section 3.2](#) are not part of the Geneve Packet.
- o Geneve Header: is described in [\[I-D.ietf-nvo3-geneve\] section 3.4](#). The Geneve Header may contain zero or more Geneve options.
- o Geneve Payload: designates the data carried by a Geneve Packet.

[[I-D.ietf-nvo3-geneve](#)]. In [[I-D.ietf-nvo3-geneve](#)] [section 3.1](#) and [section 3.2](#), the Geneve Payload would be the Inner Ethernet Header, the Payload and the Frame Check Sequence.

- o Geneve Fix Header: The Geneve Header without any Geneve Options.
- o Geneve Security Policies (GSP):
- o Geneve Security Policies Data Base (GSP DB):
- o Geneve Security Association (GSA):

Migault

Expires December 29, 2017

[Page 3]

---

Internet-Draft

Geneve Security Architecture

June 2017

- o Geneve Security Association Data Base (GSA DB):
- o Geneve Security Options (GSO): A security option defined for Geneve. Currently the security options that have been defined are GAO or GEO.
- o Geneve Authentication Option (GAO): Geneve Option that describes how to authenticate the Geneve Header as well as part of the Geneve Payload. This option is described in [[I-D.mglt-nvo3-geneve-authentication-option](#)].
- o Geneve Encryption Option (GEO): Geneve Option that describe how to encrypt Geneve Options as well as a part of the Geneve Payload. GEO is defined in [[I-D.mglt-nvo3-geneve-encryption-option](#)].
- o Geneve Security Module: an implementation responsible to enforce the security of Geneve Packets.

#### [4.](#) Architecture Overview

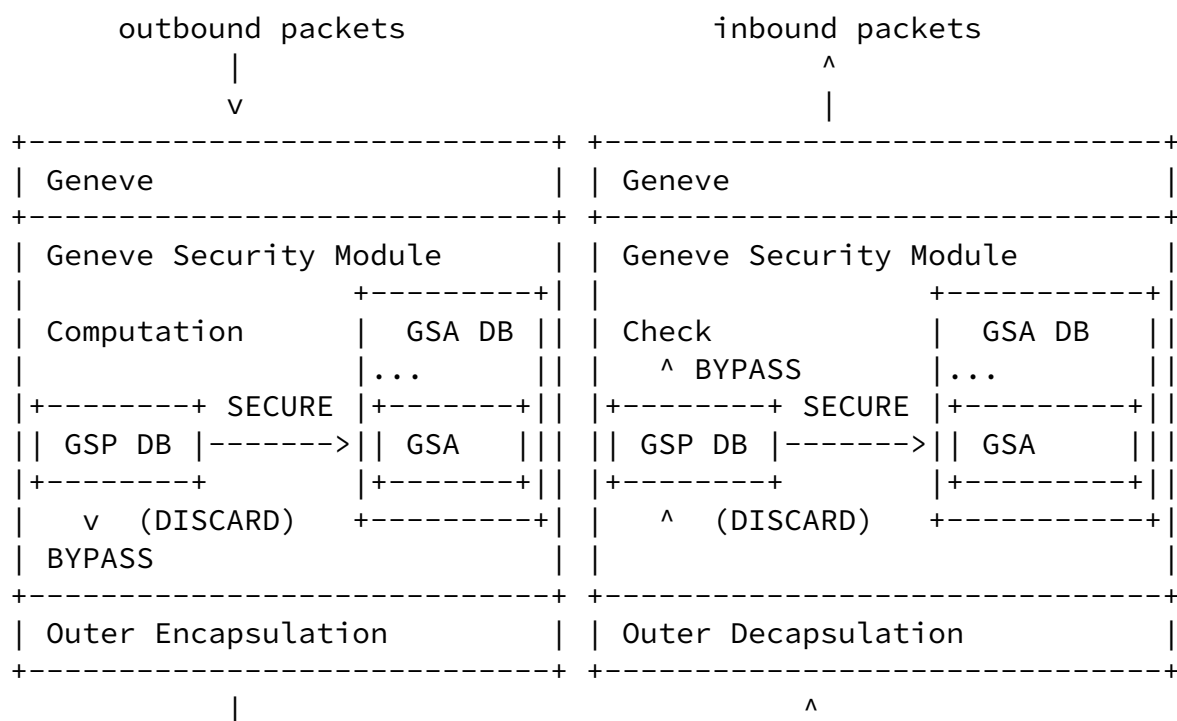
The Geneve Security Architecture is represented in figure Figure 1. Geneve security is enforced by the Geneve Security Module. The Geneve Security Policies (GSP) define which which flows inside a virtual network needs to be secured by associating a action SECURE, BYPASS or DISCARD to each Geneve Packet. When a Geneve Packet is tagged as SECURE, the GSP provides specific structures known as Geneve Security Associations (GSA) that describe how the Geneve Packet MUST be secured. Typically, the GSA defines the type of option (Geneve Authentication Option (GAO) or the Geneve Encryption

Option (GEO) to be computed or validated, as well as the necessary material such as the appropriated counters, the necessary keys to compute and validate the GS0. GSP and GSA are respectively stored in GSP Database (GSP DB) and GSA Database (GSA DB).

For outbound traffic, the Geneve Security Module receives a non secured Geneve Packet and is responsible to secure that Geneve Packet with the appropriated GS0s - as defined by the GSP/GSAs. Once the GS0 have been added, Outer Encapsulation is performed as described in [[I-D.ietf-nvo3-geneve](#)] i.e. the Geneve Packet is being encapsulated with Outer Ethernet / Outer IPv4 or IPv6 / and Outer UDP.

For inbound traffic, the Geneve Security Module defines whether a incoming Geneve Packet must be secured or not as defined by the GSP. If a Geneve Packet does not have to be secured, any GS0 found is ignored. Otherwise, the Geneve Security Module validates each GS0, and check the validated GS0s are conformed to the defined GSP. The last step is necessary to make sure that in addition to valid security options, the expected GS0 were encountered.

This document assumes that all nodes GSP DB and GSA DB are appropriately provisioned by the control plane.



---

Network

Figure 1: Geneve Security Architecture

## 5. Geneve Security Policies Database

The GSP DB contains a list of GSP that associates a Geneve Packet with a specific action BYPASS, DISCARD, SECURE.

The matching between a Geneve Packet and an action is performed through Selectors. These Selectors associated to specific values defined whether a Geneve Packet match a given GSP. As GSO may result in encrypting a Selector, a GSP lookup is always performed with a "clear text" Geneve Packet. More specifically, the GSP lookup for a Geneve Packet associated with the SECURE action is performed before the GSO is being added or after the GSO has been validated. For outbound Geneve Packet, a GSP DB look up is performed using the Selectors' value before the GSO is computed. In that case, the GSP will even provide the required structure to generate the GSO. On the other hand, for incoming traffic, the GSO is identified by an identifier carried by the Geneve Packet, a GSP look up is performed once the GSO has been validated / decrypted. As a consequence, the same GSP DB is shared by the sending and the receiving Geneve Element.

When BYPASS is selected, then the Geneve Security Module forwards the matching Geneve to the next layer. As represented in Figure 1, the next layer of an outbound Geneve Packet is the Outer Encapsulation while the next layer of an incoming Geneve Packet is the Geneve layer. When DISCARD is selected, the Geneve Security Module is expected to drop the matching Geneve Packet. When a SECURE action is selected the associated GSAs MUST be provided. For outbound Geneve Packet, the GSAs provided will be used in order to appropriately generate the GSO. On the other hand, for incoming Geneve Packet, the GSAs are returned so the Geneve Security Module can validate the GSO present in the Geneve Packet are conform to the GSP.

It is worth noting that for incoming Geneve Packet, those not tagged as BYPASS or DISCARD are by default considered as tagged as SECURE. This means that the GSP DB may be split into sub databases that

contains GSP associated to a specific action. GSP DB (DISCARD/BYPASS) may contain all GSP associated to the DISCARD and BYPASS rules while GSP DB (SECURE) contains all GSP associated to the action SECURE. By doing so, an incoming Geneve Packet may be associated to the SECURE action without performing a lookup on GSP DB (SECURE). This does not prevent the Geneve Security Module from validating the GSO found in the incoming Geneve Packet, as these GSO are carrying a specific Identifier. On the other hand, the GSP DB (SECURE) MUST be looked up in order to validate that all GSO defined by the security policies have been appropriately validated.

## [5.1.](#) Selectors

The Selectors are the elements read from the packet in order to match a GSP. When a Selector is expected to be found in the Geneve Packet, the Selector values that match the condition are indicated with a range or a list of matching values. For clarity, this document uses ANY to indicate the full range. When the Selector may not exist or may not be accessible and must be ignored to evaluate the matching condition, it is qualified of being OPAQUE.

Geneve Header Selectors:

- o Geneve Version (2 bits): The version of the Geneve Version. This field is always present and MUST be specified. When all Geneve Version are associated to the same GSP, then all values must be specified with ANY = [0, ..., 4].
- o OAM bit (1 bit): The indication of an OAM indication. When OAM and non OAM traffic is associated to the same GSP, then all values must be indicated with ANY = [0, 1].

- o Critical bit ( 1 bit): indicates the presence of a critical option. When the presence of a critical option or its absence are associated to the same GSP, then all values must be indicated with ANY = [0, 1]
- o Rsv (6 bits): Currently [[I-D.ietf-nvo3-geneve](#)] specifies the field is set to zero by the sender and ignored by the receiver. According to these rules, the sender is expected to DISCARD any

non zero values and the receiver is expect to indicate all these values in its GSP.

- o Protocol Type (16 bits): indicates the type of the Geneve Payload. It is likely that only a few types will be specified for matching.
- o VNI: indicates the virtual network identifier. It is also likely that only a small set of VNI values will be provisioned per switches.
- o Reserved (8 bits): (see Rsv)
- o Geneve Options Class - Type List: This fields specifies the Geneve Options that MUST be present. The absence of one of these option result in discarding the Geneve Header. When the presence or absence of a specific Geneve Option has no impact for the GSP selection, the value is set to OPAQUE as they may not be any options.

Additional Selectors are considered within the Geneve Payload. The Selectors provided below are expected to enable different GSP according to the protection of the traffic. Typically, the Geneve overlay network may protect differently traffic that is already protected by the tenants with IPsec, DTLS/TLS, or SSH.

- o Next Header (IPv6) / Protocol (IPv4) (8 bits): For IPv6 this field indicates the presence of an IPv6 Option or the transport layer used after the IPv6 Header. For IPv4 packets, the protocol indicates the layer after the IPv4 Header. This field is typically used to indicate whether IPsec/AH (51), IPsec/ESP (50), TCP (6) or UDP (17) is used. Next Header is a mandatory field and is expected in any IP header. When the matching condition does not consider the Next Header or Protocol number than ANY = [0, ..., 65535] is expected. When non IP packet are expected, OPAQUE is expected.
- o Port Source is typically used to determine how the tenants traffic is being protected by TLS or DTLS. Ports associated to TLS are expected to be 443 https, 636 ldaps, 989 ftps-data, 990 ftps, 992 telnets, 993 imaps, 994 ircs, 995 pop3s, 5061 sips, 22 ssh/scp.

Note that not all transport are associated with a port number.



When only transport layers with port numbers are expected to be used (such as TCP or UDP) and the matching condition does not consider the port numbers, ANY = [0, ..., 65535] is expected. When traffic may not have port numbers - such as ICMP traffic, OPAQUE is expected.

- o Port Destination: (see Port Source)

## [5.2.](#) Geneve Security Policies

Geneve Security Policies are unidirectional. A GSP is composed of:

- o Selectors that express a matching condition
- o Action that defines if the Geneve Packet MUST be DISCARDED, BYPASSED or SECURED. When the associated action is SECURE, then the GSP associates an ordered list of GSA. The GSA contains the description and the necessary material to perform the SECURE action.

The GSP DB is an ordered list of GSP.

## [5.3.](#) Geneve Security Policies Example

According to [[I-D.ietf-nvo3-geneve](#)], the associated Geneve Version is 0, a sender MUST set Rsv and Reserved to zero. When the sender only supports [[I-D.ietf-nvo3-geneve](#)], it may performed a sanity check for its outbound packets. The rules can be places at the beginning of the GSP DB.

Selector	Value	Action
Geneve Version	[1 ... 4] (non-zero)	DISCARD
OAM	[0,1] (ANY)	
Critical	[0,1] (ANY)	
Rsv	[0, ... ,63] (ANY)	
Protocol	[0, ... , 65535] (ANY)	
VNI	[0, ... , 16777215] (ANY)	
Reserved	[0, ... , 255] (ANY)	
Geneve Options	OPAQUE	
Next Header	[0, ... , 255] (ANY)	
Port Source	OPAQUE	
Port Destination	OPAQUE	
Geneve Version	[0 ... 4] (ANY)	DISCARD
OAM	[0,1] (ANY)	
Critical	[0,1] (ANY)	
Rsv	[1, ... ,63] (non-zero)	
VNI	[0, ... , 65535] (ANY)	
Reserved	[0, ... , 15] (ANY)	
Geneve Options	OPAQUE	
Next Header	[0, ... , 255] (ANY)	
Port Source	OPAQUE	
Port Destination	OPAQUE	
Geneve Version	[0 ... 4] (ANY)	DISCARD
OAM	[0,1] (ANY)	
Critical	[0,1] (ANY)	
Rsv	[1, ... ,63] (ANY)	
VNI	[0, ... , 65535] (ANY)	
Reserved	[1, ... , 15] (non-zero)	
Geneve Options	OPAQUE	
Next Header	[0, ... , 255] (ANY)	
Port Source	OPAQUE	
Port Destination	OPAQUE	

Figure 2: Example 1: Geneve Security Policy for [I-D.ietf-nvo3-geneve] compliance (sender)

By default a Geneve Security Module may DISCARD any Geneve packet that have no matching This is indicated by the following GSP at the end of the GSP DB.

Selector	Value	Action
Geneve Version	[0 ... 4] (ANY)	DISCARD
OAM	[0,1] (ANY)	
Critical	[0,1] (ANY)	
Rsv	[0, ... ,63] (ANY)	
Protocol	[0, ..., 65535] (ANY)	
VNI	[0, ..., 16777215] (ANY)	
Reserved	[0, ..., 255] (ANY)	
Geneve Options	OPAQUE	
Next Header	[0, ..., 255] (ANY)	
Port Source	OPAQUE	
Port Destination	OPAQUE	

Figure 3: Example 2: Geneve Security Policy for [I-D.ietf-nvo3-geneve] compliance (sender)

The example below details a GSP that proceeds to a specific treatment to the traffic between tenant using ESP. The specific treatment could typically only authenticate the Geneve Packet or partially encrypt the Geneve Payload, in order to only hide the Inner headers - including the ESP header - up to the ESP payload.

In the example, the GSP apply the same GSAs whatever the Geneve Header informations are. More specifically, all virtualized network share the same GSAs.

Selector	Value	Action
Geneve Version	[0 ... 4] (ANY)	SECURE [GSA1, GSA2]
OAM	[0,1] (ANY)	
Critical	[0,1] (ANY)	
Rsv	[0, ... ,63] (ANY)	
Protocol	[0, ..., 65535] (ANY)	
VNI	[0, ..., 16777215] (ANY)	
Reserved	[0, ..., 255] (ANY)	
Geneve Options	OPAQUE	
Next Header	[50] (ESP)	

Port Source		OPAQUE	
Port Destination		OPAQUE	
-----			

Figure 4: Example 3: Geneve Security Policy for ESP protect traffic

## [6.](#) Geneve Security Association Database

GSA DB contains all GSAs. GSA are expected to contain all the necessary information for the Geneve Security Module to compute the GSO by both the sender and the receiver. This includes for example the cryptographic keys to encrypt (resp. authenticate) as well as to decrypt (resp. validate) the Geneve Packet. In addition, the GSA also contains parameters associated to the protection of the security option such as the anti-replay mechanisms as well as the management of that options such as its lifetime.

For outbound traffic, the concerned GSA are provided by the GSP. In this case, it is the purpose of the implementation of Geneve Security Module to provide that appropriated reference. Most likely, the appropriated GSAs will be designated using a memory address.

For inbound traffic, the concerned GSA is designated by the associated GSO with a GSO-ID. In that case the appropriated GSA is retrieved using this index.

### [6.1.](#) Geneve Security Associations

A GSA contains the following information:

- o GSO ID: The identifier of that GSA. This identifier is used by receiver to bind the appropriated GSO to the appropriated GSA. Note that when the packet is encrypted by the GSO, it may not be possible to associate the GSA using GSP.
- o GSO Protocol: The security protocol associated with the Geneve Security Option. Currently the two GSO are GAO and GEO.

When the security option includes some encryption operation, the following parameters are provided. Note that as recommended by [[I-D.ietf-ipsecme-rfc7321bis](#)], encryption is authenticated encryption.

- o GSO Encryption Algorithm: In most cases, the encryption is combined with an authentication performed with the same key.
- o GSO Encryption Key:

When the security option includes a dedicated authentication operation ( that is not part of the encryption), the following parameters are provided:

- o GSO Authentication Algorithm:

- o GSO Authentication Key:

The following parameters indicate the coverage of the security

- o GSO Payload Covered Length: the length of the Geneve Payload covered by the GSO. The expression of the length can be a number of bytes, but it may also be defined with an abstract designation. For example, a sending node may be willing to authenticate the Geneve Payload up to the ESP layer. In that case, the sending node will have to compute the corresponding Payload Covered Length. This value is only used by the sending node. The receiving node read that value from the GA0.
- o GSO Covered Geneve Options: Indicates the Geneve Options covered by the GSO. This indication is primarily necessary for the sending node and is derived from the Geneve Packet by the receiving node. It might be checked by the receiving node to validate the GSA. It might typically be expressed as a list of Geneve Options that needs to be covered by the authentication.

In order to implement the anti replay mechanisms the following parameters are provided:

- o GSO Sequence Number Size: indicates the size of the SN. This document considers a 32 bit or a 64 bit length.

- o GSO Last Received Packet: that designates the Sequence Number last sent or received packet.
- o GSO Anti Replay Window: that indicates the minimum acceptable value of the Sequence Number. Any Geneve Packet with a lower SN MUST be rejected. Such SN value is usually derived from the Last Received Packet - Anti Replay Windows.

In order to check the conformity with the GSP:

- o GSO Selectors: The selectors are provided so the receiver can check the Geneve Packet protected by the GSO is conform to the GSP. In other words a valid GSO is not sufficient for the Geneve Packet to be forwarded to the upper layers. Note that the Selectors MUST match the Geneve Packet associated to the GSA before the GSO is built for outbound Packets. For inbound Geneve Packet the Selectors are those that corresponds to the Geneve Packet after the GSO has been validated/decrypted. Selectors are mostly expected to be used by the GSA for incoming Geneve Packet, in order to check the GSA is conform with its GSP.
- o GSA Life time:

## [7.](#) Geneve Security Module Packet Processing

This section assumes that the GSA is valid. Invalid GSA MUST be deleted or considered as non existing by either the sender or the receiver.

### [7.1.](#) Outbound Geneve Processing

- o The Geneve Security Module consults the GSP DB to determine the GSP associated to the Geneve Packet.
  - \* When a Geneve Packet is DISCARD, the Geneve Packet is dropped.
  - \* When a Geneve Packet is BYPASS, the Geneve Packet is directly forwarded to the lower layers for the outer encapsulation.
  - \* When a Geneve Packet is SECURE, the GSP returns one or multiple Geneve Security Association (GAS) of the Geneve Security

Association Database (GSA DB). GAS contains the necessary material to compute the GSO for outbound Geneve Packet. When multiple GAS are returned, GAS are applied in the order they are provided. Each computed GSO carries a unique GSA-ID, so the receiver can check the corresponding GSO without performing a GSP DB lookup.

- \* When no matching is found, the Geneve Packet is DISCARDED
- o Geneve Packet is forwarded to the lower layers for the Outer Encapsulation.

## [7.2.](#) Inbound Geneve Packet Processing

For inbound Geneve Packets:

- o The Geneve Security Module checks the Geneve Packet is associated to a DISCARD or a BYPASS GSP.
  - \* If a match occurs the Geneve Packet is either DISCARDED or BYPASSED to the Geneve layer.
  - \* Otherwise the Geneve Packet is expected to be SECURED and processed as such by the Geneve Security Module.

When the Geneve Packet is believed to be SECURED.

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

- o The Geneve Security Module inspects the Geneve Header for GSO in a network order and proceeds as follows:
  - \* The Geneve Security Module extracts the GSA-ID of the GSO.
  - \* The Geneve Security Module performs a GSA DB lookup based on the GSA-ID to retrieve the GSA associated to the Geneve Packet.
    - + If the GSA DB the GSO, the SO is skipped and the Geneve Security Module continue wity the next GSO. In this case, the GSO is treated as a unexpected geneve option.

- \* The Geneve Security Module validates the Geneve Security Option against the GSA. If the validation does not succeed, the Geneve Packet is discarded.
- \* The Geneve security Module validates the Geneve Packet – once the GSO process has been performed – is conformed with the GSP by checking the resulting Geneve Packet matches the Selectors provided in the GSA.
  - + If the validation is successful, the Geneve Security Module associates the GSA-ID with a validated status in the security context. For this reason it is important to match the GSA Selector with the appropriated Selectors value. In case multiple GSO are combined, the Selectors of the GSA MAY differ from those used for the GSP DB matching.
  - + If a mismatch occurs the Geneve Packet is dropped.

When all Geneve Security Options have been validated, 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. Note that the receiver and the sender MUST have the same GSA-IDs, however, computation and validation are processed in a different order.

## [8.](#) IANA Considerations

There are no IANA consideration for this document.

## [9.](#) Security Considerations

## [10.](#) Acknowledgment

## [11.](#) References

### [11.1.](#) Normative References



- [I-D.ietf-ipsecme-rfc7321bis]  
Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", [draft-ietf-ipsecme-rfc7321bis-06](#) (work in progress), June 2017.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

## 11.2. Informational References

- [I-D.ietf-nvo3-encap]  
Boutros, S., Ganga, I., Garg, P., Manur, R., Mizrahi, T., Mozes, D., and E. Nordmark, "NVO3 Encapsulation Considerations", [draft-ietf-nvo3-encap-00](#) (work in progress), June 2017.
- [I-D.ietf-nvo3-geneve]  
Gross, J., Ganga, I., and T. Sridhar, "Geneve: Generic Network Virtualization Encapsulation", [draft-ietf-nvo3-geneve-04](#) (work in progress), March 2017.
- [I-D.mglt-nvo3-geneve-authentication-option]  
Migault, D., "Geneve Authentication Option", July 2017, <<https://tools.ietf.org/html/I-D.ietf-nvo3-geneve-authentication-option-00>>.
- [I-D.mglt-nvo3-geneve-encryption-option]  
Migault, D., "Geneve Encryption Option", July 2017, <<https://tools.ietf.org/html/I-D.ietf-nvo3-geneve-encryption-option-00>>.
- [I-D.mglt-nvo3-security-requirements]  
Migault, D., "Geneve Security Requirements", July 2017, <<https://tools.ietf.org/html/I-D.mglt-nvo3-security-requirements-00>>.

Author's Address

Daniel Migault

Email: [daniel.migault@ericsson.com](mailto:daniel.migault@ericsson.com)

