SAI IPSEC API Proposal

High Level Design Document

# Intel IPSEC SAI proposal in addition to Arista PR #1206

# Scope



## SA Domain programming:

This is a proposed extension to the IETF RFC4303 feature set and its purpose is to allow a switch or a NIC to support multiple IPsec SA *domains*.

* 1. An SA Domain is specified in the IPSEC SA entry. The data plane packets accessing the SA entry will also have domain ID. The SA domain check ensures that only the permitted data packets that originate from the same domain ID (tenant network) can be encrypted or decrypted using this SA .
  2. Our understanding is there can be multiple SA domains, one per Control plane or one per Tenant.
  3. The SA domain check is enforced for packets that need to be encrypted (such as packets coming from the Host in case of a NIC) by identifying the Source of the packet belonging to a Tenant (Source port based identification). When the packets need to be decrypted ( such as packets coming from the wire and going towards Tenant), the SA Domain is identified based on SPI + other fields in L2 & L3 header that are in clear (such as Destination IP address + Destination MAC).
  4. Add Domain id attribute to SA creation

8

8

* 1. For devices that do not support multiple SA domains, a Global SA Domain can be configured. The HW can ignore the Domain information.

## SA Lookup Table Programming:

When the packets are sent from Host or received from the Wire, the Device must be able to select the right SA Index to Encrypt or Decrypt the packet.

In Tunnel Mode this is specified as part of the PR #1206

**For Transport Mode**

This would require ACL rules and Action to identify the SA Index

At the minimum this requires that we program an ACL Table entry to match on Source of the Packet + Destination IP + Destination MAC or a flow based 5 Tuple to identify the right SA Index and SA Domain for Encrypt operations.

For Decrypt the IPSec Tunnel Attributes for the Clear IP header itself can be used for Identifying the SA Domain and SAI Index.

We propose the following action to identify the SA Domain and SA Index for ACL Object.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | /\*\* | |  | \* @brief ACL Action Type | |  | \*/ | |  | typedef enum \_sai\_acl\_action\_type\_t | |  | { |  |  | | --- | | \* @type sai\_acl\_action\_data\_t sai\_object\_id\_t | |  | \* @flags CREATE\_AND\_SET | |  | \* @objects SAI\_OBJECT\_TYPE\_IPSEC\_FLOW\_SA\_INDEX  \* @objects SAI\_OBJECT\_TYPE\_IPSEC\_FLOW\_SA\_DOMAIN | |  | \* @default disabled | |  | \*/ | |  |  |   SAI\_ACL\_ACTION\_TYPE\_IPSEC\_FLOW | |
|  |  | |