IPsec in BGP model
(draft-ietf-idr-bgp-model-14)

IETF-114
Philadelphia, July 26, 2022

Susan Hares and Jaehoon (Paul) Jeong
BGP Peers

Secure Link with IP sec
BGP Model Use – in peer group structure

container secure-session { when "./secure-session-enable = 'true'";
  description
    "Container for describing how a particular BGP session is to be secured.";

  choice option {
    case ao {
    }
    case md5 {
    }
    case ipsec {
      leaf sa {
        type string;
        description
          "Security Association (SA) name.";
      }
    description
      "Currently, the IPsec/IKE YANG model has no grouping defined that this model can use. When such a grouping is defined, this model can import the grouping to add the key parameters needed to kick off IKE.";
    }
  description
    "Choice of authentication options.";
}
BGP Requirements

• Configuration – with rotation of keys
• Operational state
Motivation to Interface to IPsec for BGP over IPsec

• The scenarios are between two BGP routers as follows:
  • The type of IPsec connections between BGP routers can be:
    • within a trusted cloud (same administrative domain, same trust cloud),
    • across a physically secure private link,
    • across the open Internet (where attacks happen).

• There needs to have an Interface to IPsec Management for BGP Routers.
  • This interface can facilitate the IPsec Session Management between BPG Peers.
  • I2NSF is a good candidate to provide such an interface to BGP.
BGP Gateways can establish SAs with their peers with the help of Security Controller in either an IKE way or an IKE-less way in RFC 9061.

RFC 9061: A YANG Data Model for IPsec Flow Protection Based on Software-Defined Networking (SDN)
RFC 9061 can be used for the IPsec interface for BGP over IPsec.

RFC 9061: A YANG Data Model for IPsec Flow Protection Based on Software-Defined Networking (SDN)

IPsec Management for BGP with RFC 9061

- BGP routers can be regarded as NSFs.
- We can run either IKE or IKE-less approach.
- With IPsec sessions between BGP routers, BGP messages can be protected, such as Path Attributes (e.g., AS_PATH and NEXT_HOP).
Open Discussion

• Do we need to extend RFC 9061 for the IPsec interface for BGP over IPsec?

• What I2NSF YANG data models can be made for this extension for IPsec in BGP model?

• Please suggest any ideas and opinions.
Thanks for any pointers