

Major Changes to Address IESG Discuss Points for BGP Usage for SDWAN Overlay Networks

draft-ietf-bess-bgp-sdwan-usage-25

Linda Dunbar (Futurewei)
Ali Sajassi (Cisco)
John Drake (Juniper)
Basil Najem (Bell Canada)
Ayan Barnerjee & Dave Carrel (Cisco)

March 2025

Background

- IESG moved the draft back to WG to address key issues raised by IESG
- Key Decision - Document Scope:
 - Initially planned to merge with draft-ietf-idr-sdwan-edge-discovery (protocol).
 - Early Directorate reviews recommended maintaining separate document for the use cases, requirements, the pros & cons.
- Purpose of the document (Gunter, etc.)
 - draft-ietf-bess-bgp-sdwan-usage describes the SD-WAN scenario, requirements, and justifications for BGP to control the SD-WAN.
 - Establish a baseline for discussions on SD-WAN related efforts across IETF (IDR, RTGwg, IPsecme).
 - Describe the L3 VPN services over hybrid underlay paths.
 - Note: this draft doesn't use the obsoleted RFC for IPsec L3VPN

Is the document in the scope of BESS WG?

- Purpose: to define a standardized approach to using BGP for the control plane in SD-WAN overlay networks.
- Covers: using BGP to manage L3 VPN services over hybrid underlay paths.
Per BESS WG charter:
 - Defining, specifying, and extending network services based on BGP.
 - Supporting BGP-enabled services in multi-homing scenarios for load balancing and resilience.
- BGP-based SD-WAN overlays are a growing reality, and this draft doesn't create anything new, it just standardizes how BGP & IPsec are used in SD-WAN to make deployments more consistent and interoperable.
- Options: In BESS WG or Elsewhere?

Summary of Resolutions to IESG Discuss Points

- The IPsec Tunnel Type specified in RFC5566 is obsolete. A new tunnel type is needed to represent the IPsec Tunnel underlay path (from John Scudder)
 - Made the change as below and removed IPsec tunnel type throughout the doc

“Note: The IPsec Tunnel Type specified in RFC 5566 is obsolete. To indicate that the prefixes 192.0.2.4/30 and 192.0.2.8/30 are carried using a hybrid of IPsec underlay paths, a new tunnel type, such as one designed for SDWAN-Hybrid environments, is required. The specific definition and mechanism of such a tunnel type are expected to be addressed in future specifications.”
- The spec has to be clear about what the "Encapsulation Extended Community: TYPE = IPsec" (or its replacement) is **for**, since it's clearly **not** for what RFC 9012 documents the semantics of an Encapsulation Extended Community to be (John Scudder)
 - A new SDWAN-Hybrid tunnel type in the Encapsulation Extended Community is intended to explicitly specify a hybrid tunnel that combines the secure VPN and non secure VPN (which is secured by IPsec SA)
- Why need RFC 4684 (Constrained Route Distribution)?
 - The reference to RFC4684 was removed in v-23. The updated paragraph is:
“BGP is well suited for this purpose. A Route-Reflector (RR) [RFC4456], integrated into the SD-WAN controller, has the policy governing the communication among peers. The RR ensures that BGP UPDATE from an edge only is propagated to the edges within the same SD-WAN VPN.”

Summary of Resolutions to IESG Discuss Points- cont

- Security Considerations section deserves to have a clearer description of the security model, instead of having it only embedded in the middle of Section 3.1.5. (John Scudder)
 - The updated Security Consideration now explicitly states that the security properties of the SD-WAN depend heavily on the correct configuration and operation of the Route Reflector (RR), which acts as the central control point. This includes secure communication channels, policy enforcement, and mitigation of risks associated with Internet-facing WAN ports.
- The imperative, comprehensive analysis of [BGP-OVER-TLS] is not sufficiently motivated (Roman Danyliw)
 - Removed the BGP over TLS description
- Need more description for anti-DDoS mechanism (Roman Danyliw)
 - The anti-DDoS mechanism comprises numerous components, and their detailed discussion is beyond the scope of this document

Next Step

- **Are the resolutions good enough**
- **Need another WGLC**
 - Suggested by IESG