




CONTROLLER - IKE

What? Why? Where? Who? And when?



What?

- At a high level, it provides the same function as IKE
 - *e.g. Can replace the IKE daemon on Linux while using the existing kernel IPsec.*
- DH based key exchange done through a controller
 - *All peers send their DH public value to the controller*
 - *Controller sends the list of all public values to all peers*
 - *All peers calculate a unique pairwise secret for each other peer*
 - *Synchronization is what makes this interesting!*
- Key material is exchanged along with the overlay routing data.
- No peer-to-peer messages

What ISN'T it?

- NOT a replacement for IKE. It's an alternative.
- It is NOT a 2-way tunnel attribute negotiation protocol
 - *No back and forth negotiating, but hey, we're controller based.*
- It does not (currently) provide its own secure communications to the controller

Why?

- Optimized key exchange for large controller based environments.
 - *N vs. N^2 messages*
 - *Scalable for very large networks.*
- Odd shaped networks
 - *Not everything is normal or even bi-directional*
 - *Control can traverse one network, while encrypted data traverses another.*
- Easy to add new nodes.

Where?

- Drafts

- <https://tools.ietf.org/html/draft-sajassi-bess-secure-evpn-02>
- <https://tools.ietf.org/html/draft-dunbar-bess-bgp-sdwan-usage-01>
- <https://tools.ietf.org/html/draft-dm-net2cloud-gap-analysis-04>
- <https://tools.ietf.org/html/draft-ietf-rtgwg-net2cloud-gap-analysis-02>

- IETF Mailing list (non-WG)

- sdwan-sec@ietf.org

- WG discussions

- I2NSF, BESS, IDR, RTGWWG, ...

Who?

- Authors:

- *David Carrel* <carrel@cisco.com>
- *Brian Weis* <bew.stds@gmail.com>

When?

- There are two known implementations.
 - *To be honest.. they're related*
- Further Considerations
 - *QR*
 - *SPI format*
 - *Signed DIMs*
- But the real “When” is the question for this room...