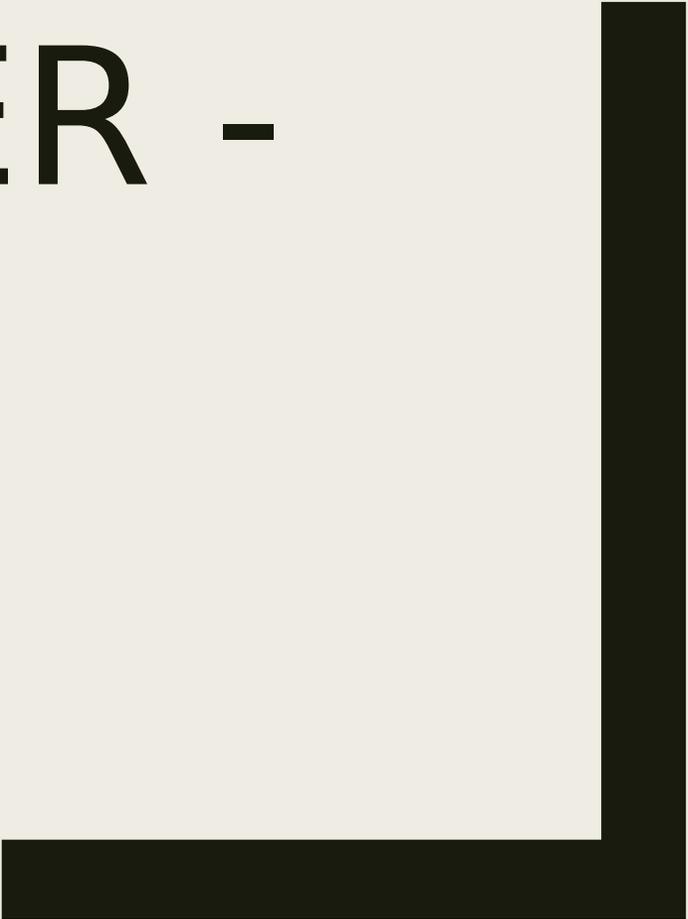




# CONTROLLER - IKE

Why mess with perfection?



# Motivation

## ■ SD-WAN

- *Everything is controller driven*
- *Full mesh IPsec*

## ■ Scalability

## ■ SD-WAN done wrong

- *Protect those keys*

## ■ Odd shaped networks

- *Not everything is normal or even bi-directional*

# What the heck is Controller-IKE

- DH based key exchange done through the controller
  - *All peers send their DH public value to the controller*
  - *Controller sends the list of all public values to to all peers*
  - *All peers calculate a unique pairwise secret for each other peer*
  - *Peers can sign their message if desired*
- No peer-to-peer messages
  - *No back and forth negotiating, but hey, we're controller based.*
- That was easy.... What could go wrong?

# The “fun” stuff

- OK, so what happens when a peer re-keys?
- What happens when 10,000 peers all re-key?
  - ... *at almost the same time?*
- What happens when a network must support more than one algorithm?
  
- With the right rules, we actually make this work.
  
- Read the draft and find out more...

# Wrapping up

- This has been just a quick introduction.
  - *We'd like to go further.*
- This draft defines a method and not a protocol.
  - *This should be embedded in a controller protocol.*
  - *Goal is to ensure controller protocols "do the right thing".*
- Further Considerations
  - *QR*
  - *Signed DIMs*
  - *Do we want a protocol?*

# Authors

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