The Problem to Solve

Modify the previously defined policy for avoiding ECMP-induced asymmetries in mult-zone/multi-site topologies to account for scenarios in which different security zones have a different as-path length on their inter-site/WAN links. Do this to ensure that traffic from S*n*Z*p* to S*m*Z*p* always prefers the path the stays within zone *p*, avoiding any firewall hops (even if that path has a much higher AS-path-length.

The Solution

Introduce additional logic into the previously established BGP policy that utilizes the BGP local-preference attribute to prioritize routes that traverse the same security-zone.

- Always prefer the path that only contains hops in the same security-zone as the sending router
  - This is the new logic, superseding all of the following rules
  - **Implemented by assigning a higher BGP local-pref to routes that:**
    - **Have ORSECZID that matches that local router, *and***
    - **Have OSSHC of zero.**
  - Implemented on the "receiving route" phase of policy implementation
- Always prefer the shortest path (as measured by AS path count)
- ***If*** equal cost paths are present, then
  - For routers with non-zero site-IDs and zone-IDs of zero, always prefer next-hops with a non-zero Zone-ID to next-hops with a zone-ID of zero.
    - This prevents the zone-zero routers from each site from considering path-A in our examples above, and only considers paths B/C
      - We never want to traverse path, A. This is the "one-firewall at each site" path, and the zone-0/transit-zone VRFs at each end don't have a consistent reflexive basis of comparison for of their own zone-ID's to that of the destination route.
  - Always prefer the path with more stateful hops in the site of the higher security-zone ("higher" of the packet's source and destination sites)
    - Equivalently: Always prefer the path with less stateful hops in the site of the lower security-zone ("lower" of the packet's source and destination sites)

Modified to account for variable-length inter-site transit paths