Network to Cloud DC (Net2Cloud) Update
Adding Inter Cloud DC related issues

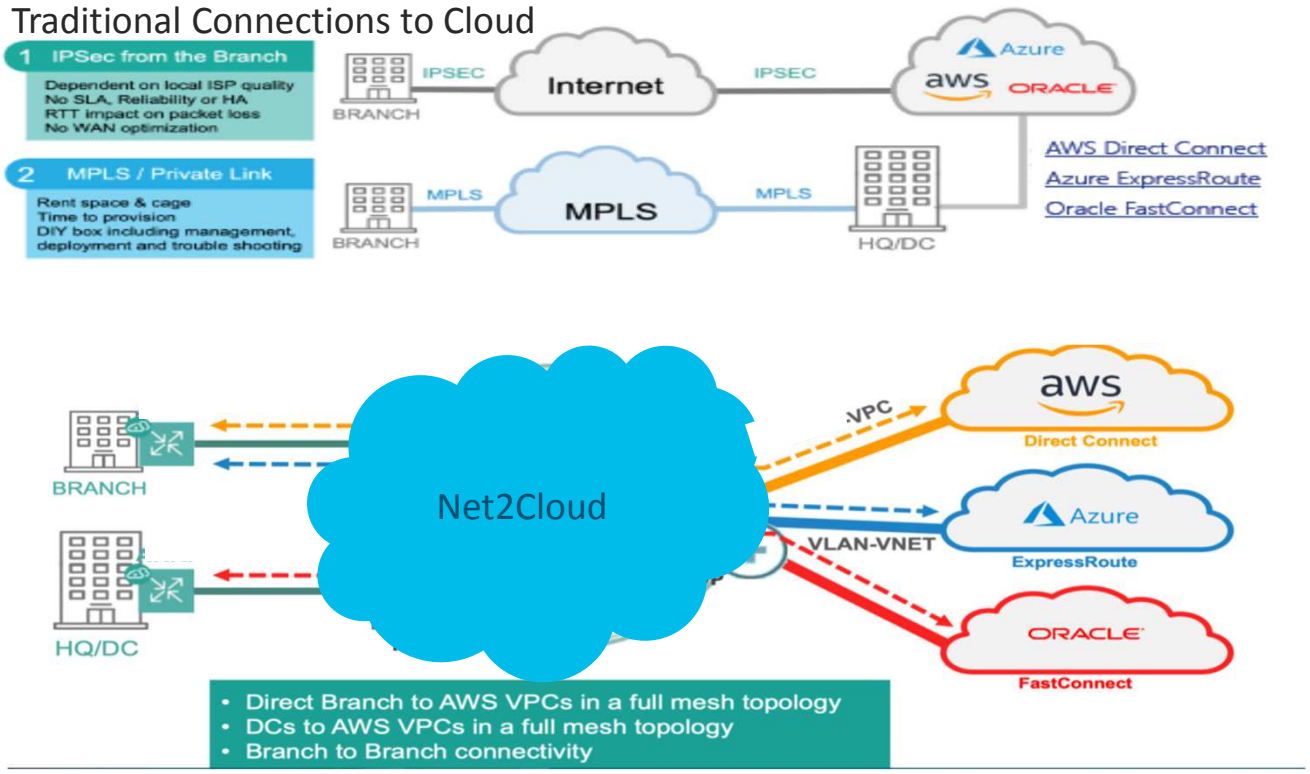
draft-ietf-net2cloud-problem-statement-05
draft-ietf-net2cloud-gap-analysis-03

Linda.Dunbar@futurewei.com
Andy Mails (agmalis@gmail.com)
Christianjacquenet@orange.com
Mehmet.toy@verizon.com

Purpose of the documents

- Identify some of the network problems associated to the network to Cloud DC and among the Cloud DCs
- Analysis IETF existing tools available and the gap
- Other problems are out of the scope

Cloud to Cloud interconnection addition



Problem Statement Update Since IETF 105

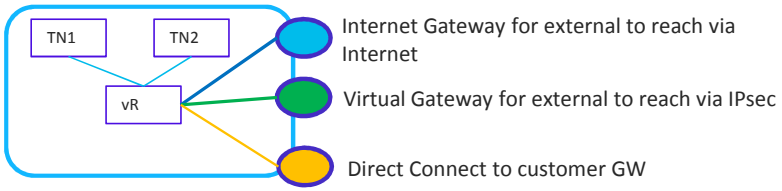
- Add a section on network characteristics of interconnecting multiple hybrid Cloud DCs.
- Add a section on Network to Cloud key characteristics:
  - Network path augmentation
  - Application based policies, which move with the applications.
  - Application ID based forwarding, instead of Destination Address based forwarding

Key requirement for Multi-cloud

- Authorization,
- how to indicate which VPC, which Vnet, and their mapping
- consistent APIs or abstractions
  - Is it possible for IETF to provide a set of YANG models as shim layer between different cloud?
- how does one Cloud DC get notified of NAT or DNS used by other Cloud DCs.
- Which DCs are connected
  - Is it necessary to have a protocol to auto discovery all the Cloud DCs being used?

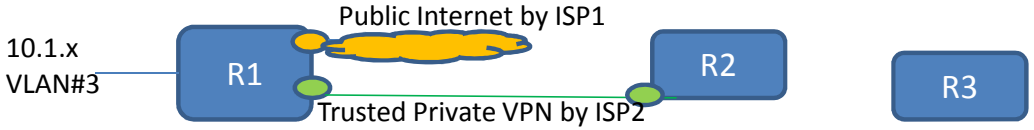
Key problems associated with Network to (and between) Cloud DCs

- Problems associated with Multiple Cloud DC Interconnection (newly added)
  - Different Cloud providers have different access method.
    - Today you have to hairpin the traffic to customer GWs
  - Different Cloud providers have different APIs for calling security functions, the NAT, etc.
- Multiple types of connections to workloads in a Cloud DCs
  - it is not visible to App in Cloud DC what type of network access is used.
- IPsec P2P doesn't scale well with Multipoint mesh connection & poor performance.
- Network to vCPE in Cloud DCs can have portion of connection unknown
- Problems of MPLS based VPN extending to Hybrid Cloud DC
  - PE might not have direct connections to Cloud DCs
  - Most Cloud DCs don't' expose their internal network. Difficult to extend MPLS VPN into Cloud DCs
  - Most Cloud Operators use Ipsec VPN to connect to their clients

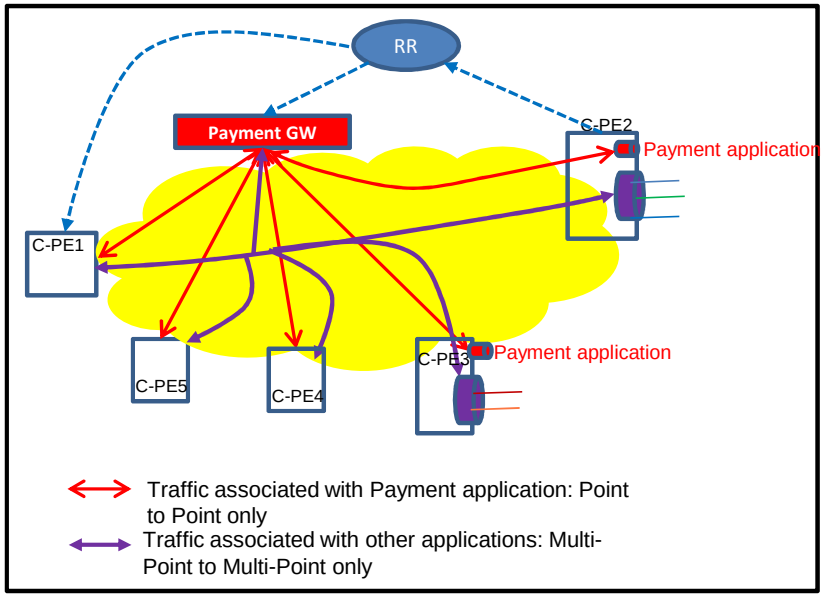


Gap analysis update since IETF 105
Tunnel-Encap

- Application Based Forwarding may require same Source IP having different forwarding topology
- Tunnel-Encap doesn't address the WAN ports properties
- To encode the IPsec information in the Tunnel Encap, it requires a lot of information (source & destination pairs)



- Need to have WAN port-based IPsec because the Loopback address and client routes are not routable in the WAN.
  - Remote nodes need to ping the WAN port to discovery failure.



Next Step

- Need more people to review and provide comments.
- Remove some text to make the key purpose of the documents more clear.