Network to Cloud DC (Net2Cloud) Problem statements and Gap Analysis Soliciting comments for WG Last Call

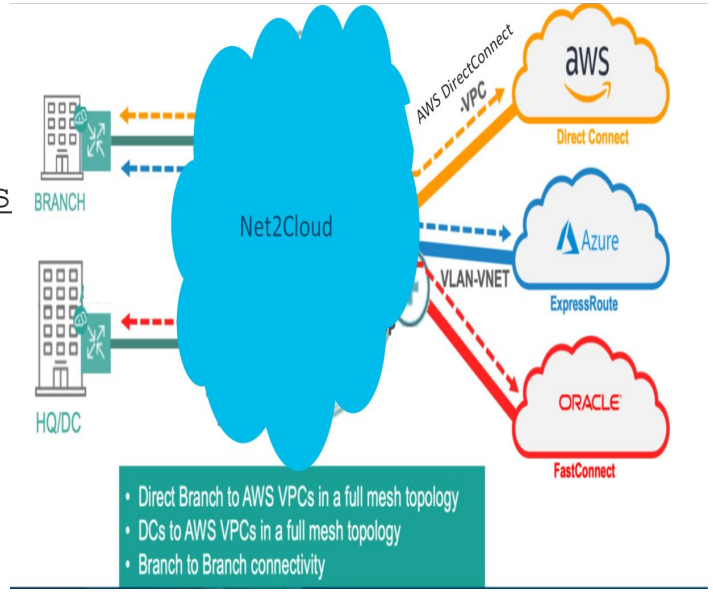
draft-ietf-net2cloud-problem-statement-10
draft-ietf-net2cloud-gap-analysis-06

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

Problem Statement Update Since IETF 106

- Removed all reference to SDWAN
- Focus on problems associated with interconnecting branch offices with dynamic workloads in Cloud DCs.
  - More on problems that need additional work in IETF Routing area.
  - Other work out of Scope
- Add a section on Network to Cloud key characteristics:
  - Network path augmentation
  - Application based policies, which follow the applications when the applications move to a different Cloud DC.
  - Application ID based forwarding, instead of Destination Address based forwarding

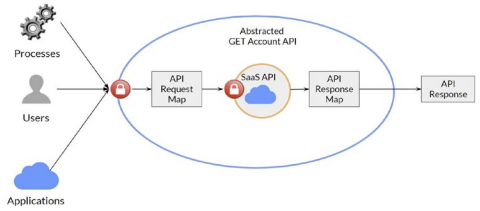
Restructured Table of Contents



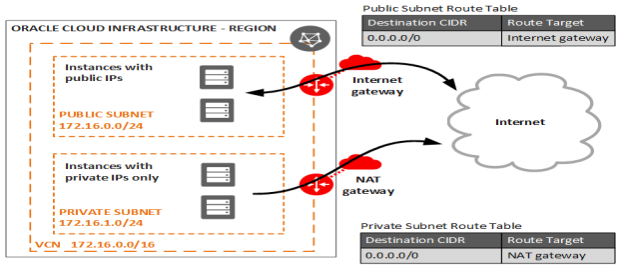
Connect the on-demand, elastic and 3rd party hosted workloads

- **Identity Management**
  - User authorization,
  - The authorization of API calls by applications from different Cloud DCs.
  - Authorization for Workload Migration, Data Migration, and Workload Management.

- **API Abstraction**
  - Desirable to have common API shim layer to manage the networks and respective security policies



- **NAT for Cloud Services**
  - Different Cloud operators support different levels of NAT functions.
  - proper configuration of NAT has to be performed in Cloud DCs and in their own on-premise DC

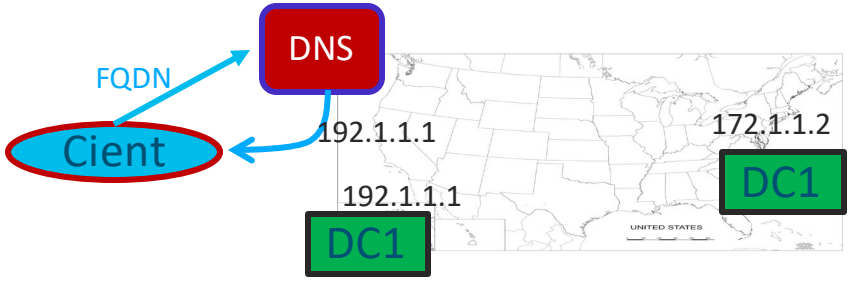


- **Cloud Discovery**
  - location of workloads and connectivity are not easily visible
  - Desirable to have tools to discover cloud services in much the same way as you would discover your on-premises infrastructure

Issues with the DNS

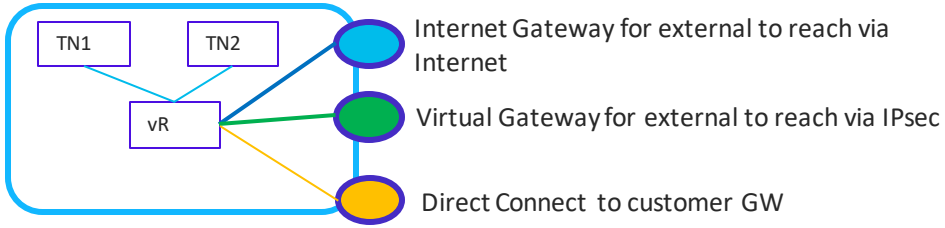
- DNS for Cloud Resources
  - Need to establish policies and rules on how/where to forward DNS queries to

    Cloud's DNS can be configured to forward queries to customer managed authoritative DNS servers hosted on-premises, and to respond to DNS queries forwarded by on-premises DNS servers.
  - Collisions can still occur. Better to use the global domain name even when an organization does not make all its namespace globally resolvable
- DNS based solution to reach App Instances in the optimal Cloud DC locations (Cloud discovery)
  - Dependent on client behavior
    - Client can cache results indefinitely
    - Client may not receive service even though there are servers available (before cache timeout) in another Cloud DC
  - No inherent leverage of proximity information present in the network (routing) layer, resulting in loss of performance
    - Client on the west coast can be mapped to DC on the east coast
  - Inflexible traffic control:
    - Local DNS resolver become the unit of traffic management



Network: Site <-> Cloud & Cloud <-> Cloud

- Problems associated with Multiple Cloud DC Interconnection
  - 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 Apps in a Cloud DC what type of network access is used.
- IPsec P2P doesn't scale well with Multipoint mesh connection & poor performance.
- unknown segments → difficult to collect end to end performance metrics
- 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

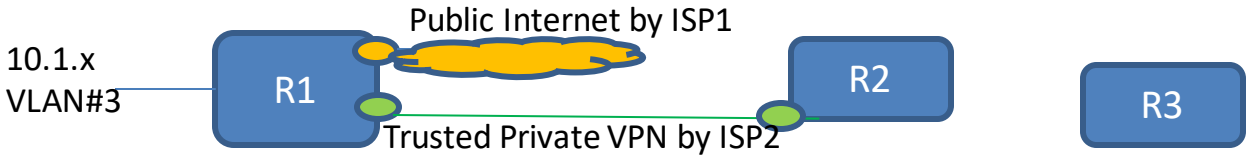


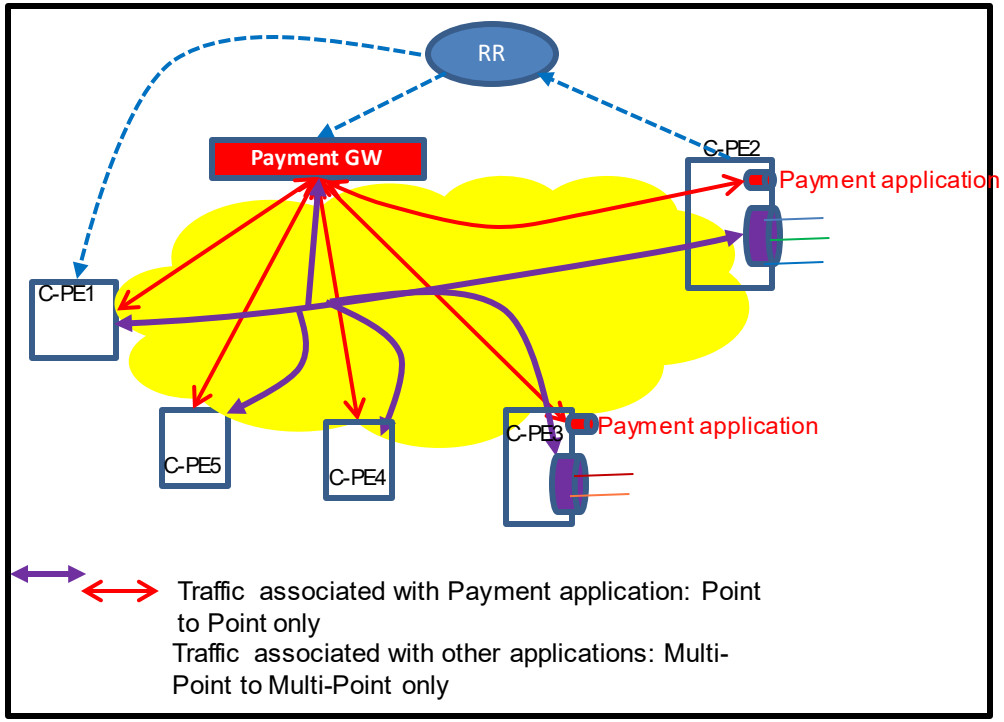
Net2Cloud Gap Analysis

Table of Contents

Gap analysis update since IETF 106

- Application Based Forwarding may require different forwarding topologies based on Application identifiers
- When a client route can be reached by either Cloud Direct connect private paths or IPsec over public network, the BGP Route Update doesn't yet have the Sub-TLV within Tunnel-Encap to indicate the following paths:
  - Private dedicated path, like DirectConnect
  - IPsec over Internet
- Doesn't yet have ways to indicate one client route can be carried by multiple underlay paths.





Gap Summary

specifically for Routing Area

- **For Accessing Cloud Resources**
  a) Traffic Path Management: when a remote vCPE can be reached by multiple PEs of one provider VPN network, it is not straightforward to designate which egress PE to the remote vCPE based on applications or performance.
  b) NAT Traversal: There is no automatic way for an enterprise's network controller to be informed of the NAT properties for its workloads in Cloud DCs.
  c) There is no loop prevention for the multicast traffic to/from remote vCPE in Cloud DCs.
  d) BGP between PEs and remote CPEs via untrusted networks.
- **Missing control plane to manage the propagation of the property of networks connected to the virtual nodes in Cloud DCs.**
- **Issues of Aggregating traffic over private paths and Internet paths**
  a) Control plane messages for different overlay segmentations needs to be differentiated. User traffic belonging to different segmentations need to be differentiated.
  b) BGP Tunnel Encap doesn't have ways to indicate a route or prefix that can be carried by both IPsec tunnels and VPN tunnels
  c) Missing clear methods in preventing attacks from Internet-facing ports

Next Step

- Request Working Group Last Call

Potential new work in Routing Area?

- Tools to indicate which Cloud VPC, which Vnet, for specific client routes (or virtual nodes within Cloud)
- Leverage of information present in the network (routing) layer to improve DNS based Cloud Discovery?
- Tools to facilitate one Cloud DC getting notified of NAT or DNS used by other Cloud DCs?