AWS re:invent Notes

Contents

[**re:invent 2016** 1](#_Toc28602149)

[AWS re: invent 2016: From One to Many: Evolving VPC Design (ARC302) 1](#_Toc28602150)

[AWS re:Invent 2016: Deep Dive: AWS Direct Connect and VPNs (NET402) 4](#_Toc28602151)

# **re:invent 2016**

# AWS re: invent 2016: From One to Many: Evolving VPC Design (ARC302)

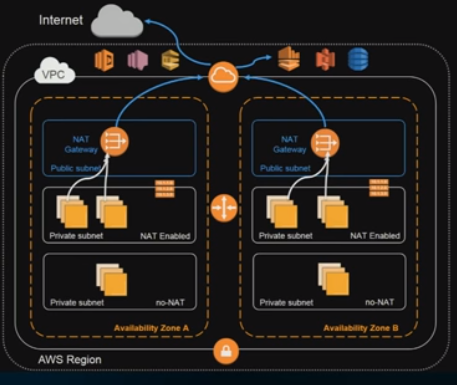
URL: <https://www.youtube.com/watch?v=3Gv47NASmU4&t=391s>

* Best practice while designing VPC
  + Go big with the VPC – go for larger CIDR block don’t think about wasting IPs
  + Subnet is not unit of segregation, thus don’t need too many subnets like in case of on-premises enterprise landscape.
  + There is no performance impact of having large number of instances within a single subnet.
  + Use security group for isolation instead of subnets – as they are robust.
  + Use tag for grouping.
  + Use subnet as container for routing policy.

One should have three subnet – public subnet, private subnet where instance can reach out to internet (egress only connectivity), private subnet tied



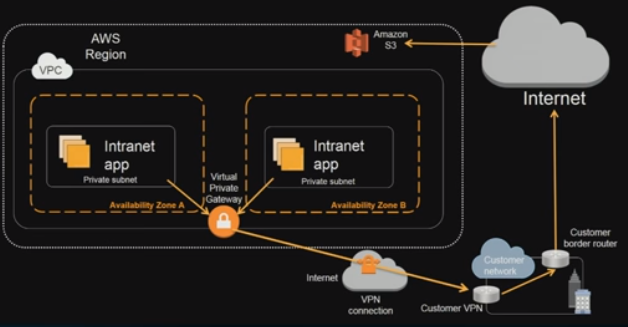
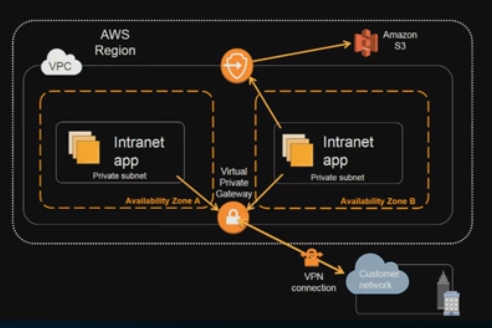
Note: Need to watch **re: invent** **NET401-Another Day, Another Billion Packets** to understand the impact of having thousands of instances within a same subnet.



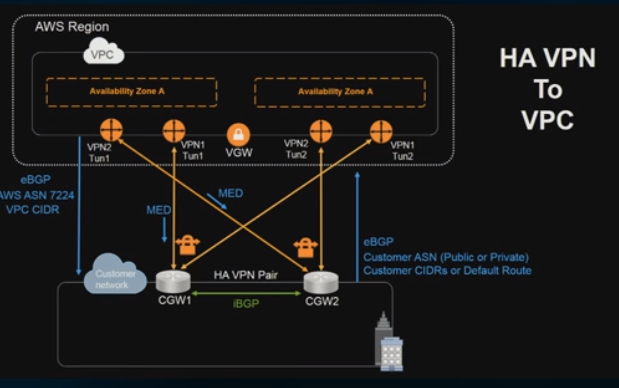
* Why we need NAT gateway instead of NAT instance?
  + To open a NAT connection, it needs a unique source ID every time it establishes an egress connection source ip in internet thus making it hard to scale this horizontally which is overcome in case of NAT gateway.
  + Requirement for a NAT gateway
    - Needs IGW to connect to internet
    - Need separate subnet – as there is NO security group that can be attached to a NAT gateway; thus, it needs a separate subnet (route-table) so that inbound traffic can be controlled.
    - Need an elastic IP address.
    - Its AZ specific , deploy NAT gateway per AZ to ensure high availability.
    - Burst to 10 Gpbs
* Pros and Corns of using NAT gateway

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| Migration of a NAT instance to NAT gateway is easy. | Does NOT provide other NAT features like – URL filtering, packet filtering, UTM, IPS etc. |
| Fully Managed | Does not supports security Groups |
| Highly available and fault tolerant – within the AZ |  |
| Supports VPC Flow Logs – one can monitor what traffic is passing through the NAT gateway |  |

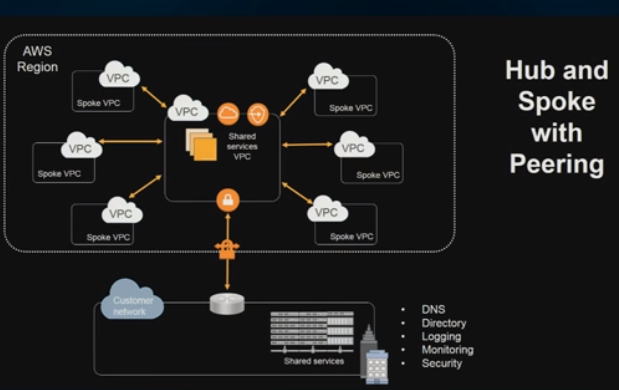
* One VPC or multiple VPC
  + To limit the blast radiuses – as it gives fine grain configuration, its advisable to have multiple VPC instead of ONE large VPC, to ensure when a large number of users are working on it in parallel they don’t override each other configurations.
  + To separate Production environment from Test and Development environment.
  + To separate out API based on regulatory and compliance requirements.
  + To separate production from disaster recovery (BPC) environment.
  + To separate domain like VPC for sales, legal, product-development, pre-sales
* How to connect publicly available services like S3 from a VPC in a most effective way.
  + One using client route through VPN connection
  + Other one using VPC endpoints – following are benefit of using VPC gateway interfaces to connect to publicly available services like s3 and DynamoDB
    - Free – no charges for VPC gateway.
    - Does not need IGW or a NAT instance to connect
    - Provide robust access control – multiple level one can enforce security
      * By creating routing table association
      * By attaching VPC Endpoint policy
      * By attaching Bucket Policy enforcing which VPCs can communicate and what actions.
      * Adding restriction using PREFIX list in security group (Create PREFIX list as it makes it more manageable).

* Connecting multiple VPCs down to the Corporate datacentre:

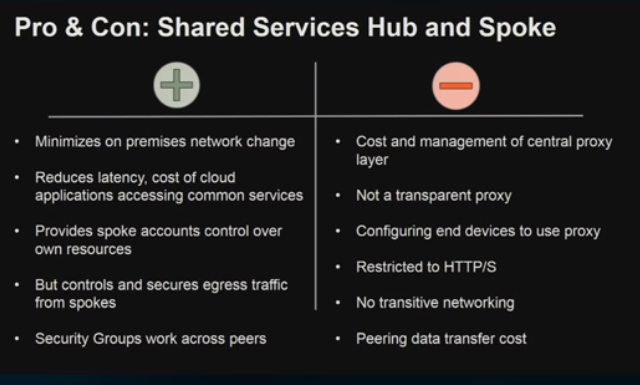


Traditional Approach: using HA VPN connection

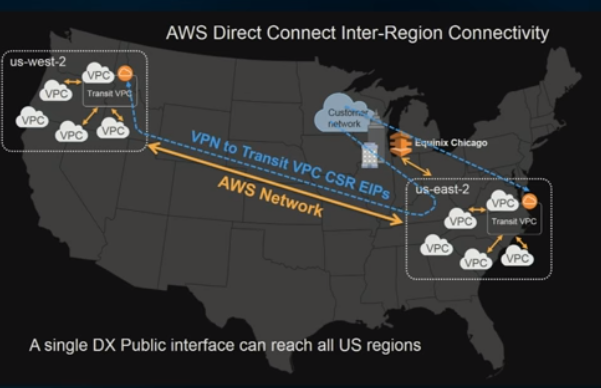


Newer Approach: Using Hub and Spoke with Peering Connections.

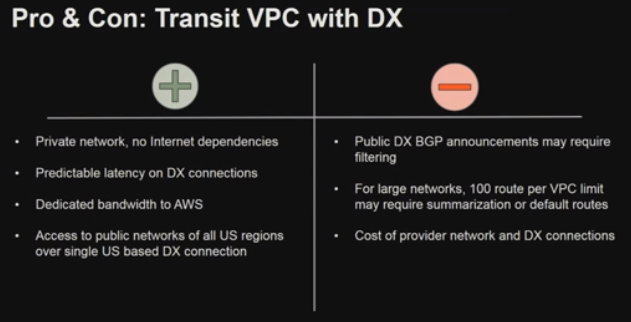
* Prop and Corns of using Hub and Spoke



* Once a direct connection is established across a single US region, using the same connection one can reach to all US region. (this cannot be achieve using private direct connect – using private direct connect one can reach out to ONLY VPC where its connected to)



* Pros and Cons: Transit VPC with Direct Connect



* Deep Dive on Direct Connect can be found under **NET402-Deep Dive: AWS Direct Connect and VPNs**.

# AWS re:Invent 2016: Deep Dive: AWS Direct Connect and VPNs (NET402)

URL : <https://www.youtube.com/watch?v=Qep11X1r1QA>