AWS-VPC-Peering , VPN & Direct Connect

VISHWANATH M S

VISHWACLOUDLAB.COM

Different Types of Connectivity to AWS

- VPC-Peering → For inter VPC connectivity within/across Regions.
- VPN → Private connection over the internet from Local Datacenter to AWS VPC
- Direct Connect → Private Connection from AWS to Local Datacenter via the private link.
- Transit Gateway → Can combine all the above connectivity

VPC – Peering

VPC-Peering Use Case

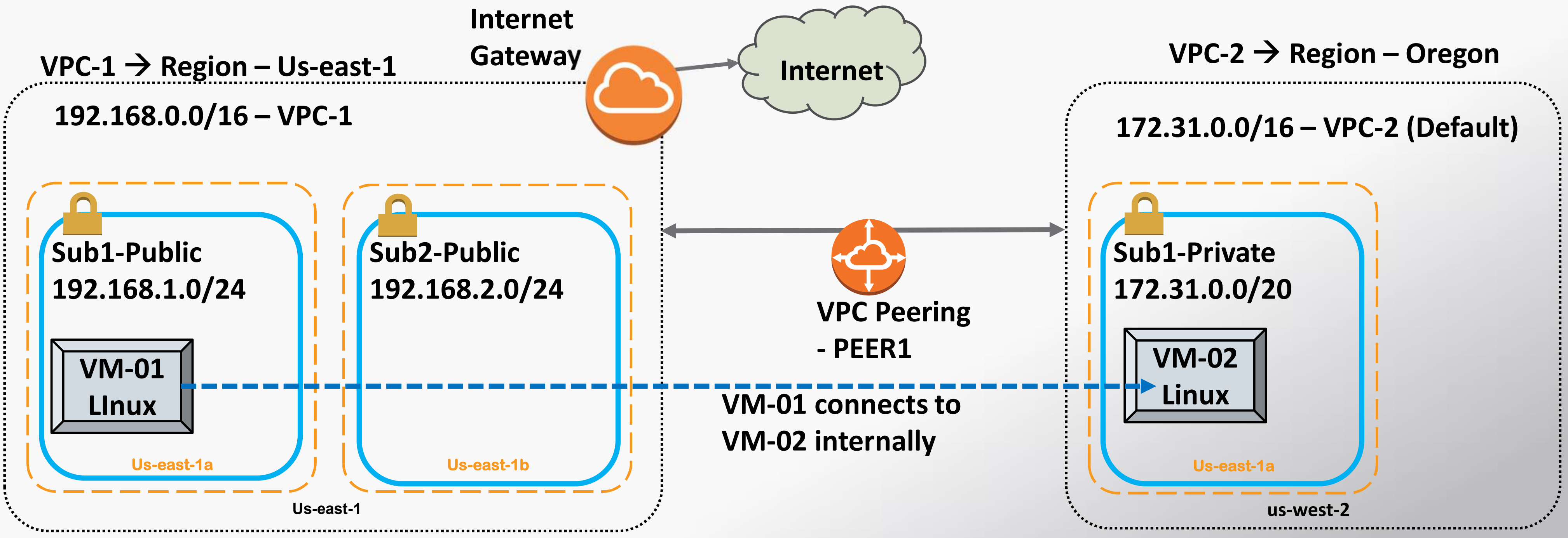
- By default 2 VPC’s in an AWS cannot talk to each other
- VPC Peering can help us connect 2 VPC’s in an AWS

- **Use Case**
  - **If we want private connection between 2 VPC’s in the same region or diff region**
  - **2 AWS customer’s now want to talk to each other over a private network**

VPC-Peering

- **Pre-requisite**
  - The Source and destination VPC should have **“DIFFERENT”** networks.
  - Eg:-- VPC-1 → 172.18.0.0/16 and
  - VPC-2 → 172.20.0.0/16
- **Type of VPC Peering Connectivity**
  - B/W 2 VPC’s within the **same Region and Same Account**
  - B/W 2 VPC’s within the **same Region and Different Account**
  - B/W 2 VPC’s with **Different Region but Same Account**
  - B/W 2 VPC’s with **Different Region and Different Account**

VPC-Peering – Demo – Setup - Details



VPC-1 → Region – Us-east-1

Internet Gateway

Internet

VPC-2 → Region – Oregon

192.168.0.0/16 – VPC-1

172.31.0.0/16 – VPC-2 (Default)

Sub1-Public
192.168.1.0/24

VM-01
LInux

Us-east-1a

Sub2-Public
192.168.2.0/24

Us-east-1b

Us-east-1

VPC Peering
- PEER1

VM-01 connects to
VM-02 internally

Sub1-Private
172.31.0.0/20

VM-02
Linux

Us-east-1a

us-west-2

Add routing entry on VPC-1 routing table
172.31.0.0/16 go via PEER1

Add routing entry on VPC-2 routing table
192.168.0.0/16 go via PEER1

VPC-Peering Limitations

- Works on IPV4 only.
- Routing of IPV6 between the VPC’s is supported only within the same Region. It could be in the same account or Different account.

Steps For VPC-Peering

1. Create VPC's on either side of the Region, one with Internet Gateway, another with either NAT gateway or no GATEWAY.
2. Create Subnets.
3. Update the Routing table of first VPC with Internet Gateway.
4. Create VM's in the respective VPC's
5. Create VPC-Peering from one of the VPC and Accept it on the other VPC.
6. Update Routing table of both the VPC with other VPC's network.

Troubleshooting issue on VPC-Peering

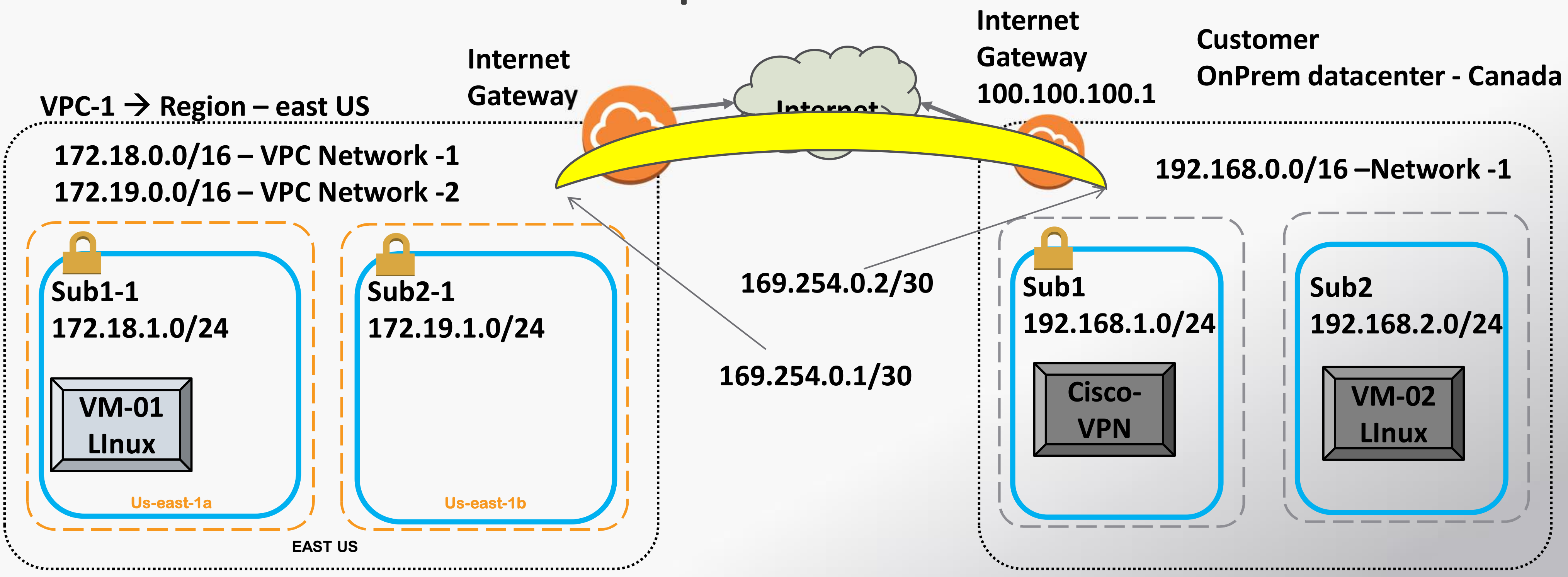
1. Verify that the VPC peering connection is in the Active state
2. Verify that the correct routes exist for connections to the IP address range of your peered VPCs through the appropriate gateway in the routing table.
3. Verify that an ALLOW rule exists in the network access control (network ACL) table for the required traffic.
4. Verify that the security group rules allow network traffic between the peered VPCs.
5. Be sure that no firewall rules block network traffic between the peered VPCs.
6. Use network utilities such as traceroute (Linux) or tracert (Windows) to check rules for firewalls such as iptables (Linux) or Windows Firewall (Windows).

VPN – Virtual Private Network

VPN Connections

- AWS Site-to-Site VPN
- AWS Client VPN
- AWS VPN CloudHUB
- Third party software VPN appliance

VPN – Demo – Setup - Details



VPC-1 → Region – east US

Internet
Gateway

Internet

Internet
Gateway
100.100.100.1

Customer
OnPrem datacenter - Canada

172.18.0.0/16 – VPC Network -1
172.19.0.0/16 – VPC Network -2

192.168.0.0/16 –Network -1

Sub1-1
172.18.1.0/24

VM-01
LInux

Us-east-1a

Sub2-1
172.19.1.0/24

Us-east-1b

EAST US

169.254.0.2/30

169.254.0.1/30

Sub1
192.168.1.0/24

Cisco-
VPN

Sub2
192.168.2.0/24

VM-02
LInux

Add routing entry on VPC-1 routing table
192.168.0.0/16 go via VPN

Add routing entry on VPC-2 routing table
172.18.0.0/16 go via VPN
172.19.0.0/16 go via VPN

VPN – Virtual Private Network

- Routing Updates in a VPN
  - Static
    - Means we would configure the Routing table for the destination networks Manually.

    (Similar to VPC-Peering)
  - Dynamic
    - Means we would be configuring an Dynamic Routing Protocol (BGP in this case) for the networks to be updated automatically in the Routing table of VPC and Local on prem Datacenter VPN box.
    - We need to provide an ASN (Autonomous System Number) for a BGP peering from VPC to onprem VPN box.

Creating VPN – Virtual Private Network

- 3 Major steps involved in creating VPN on AWS.
  - Configure Customer Gateway
  - Configure Virtual Private Gateway
  - Configure VPN

Troubleshooting issue on VPN

1. Check if the VPN connection is ACTIVE.
2. Check Network ACL in your VPC
3. Verify the security group rules.

Direct Connect

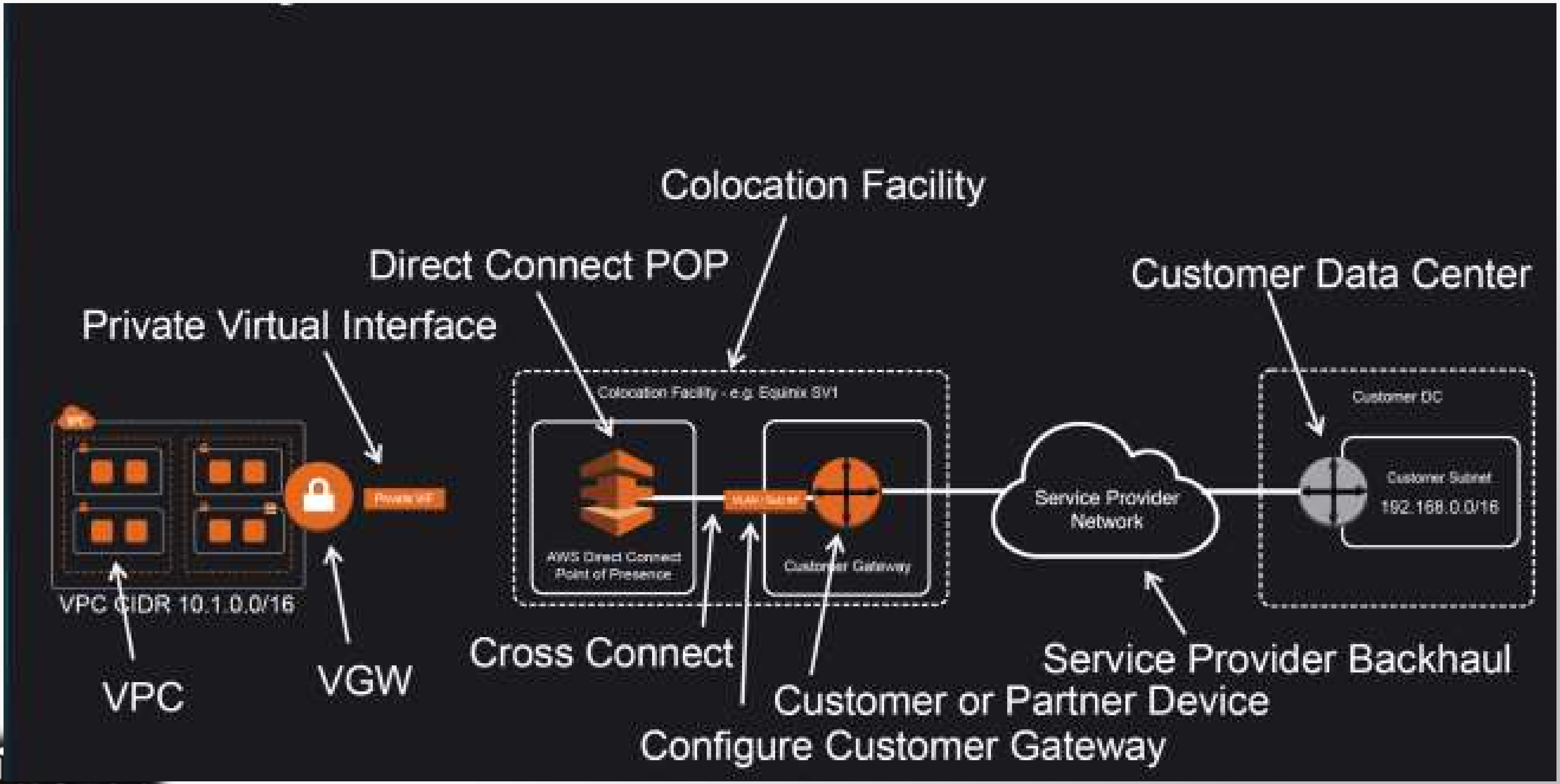
What is Direct Connect

- AWS Direct Connect links your internal network (ONPREM Datacenter) to an AWS Direct Connect location(On AWS) over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable.
- With one end of the cable connected to your router (OPREM Datacenter), the other end to an AWS Direct Connect router(Virtual Router).

Direct Connect Advantages

- **Consistent Network Performance**
- **AWS Services Compatibility**
- **Private Connectivity to AWS VPC**
- **Elastic**

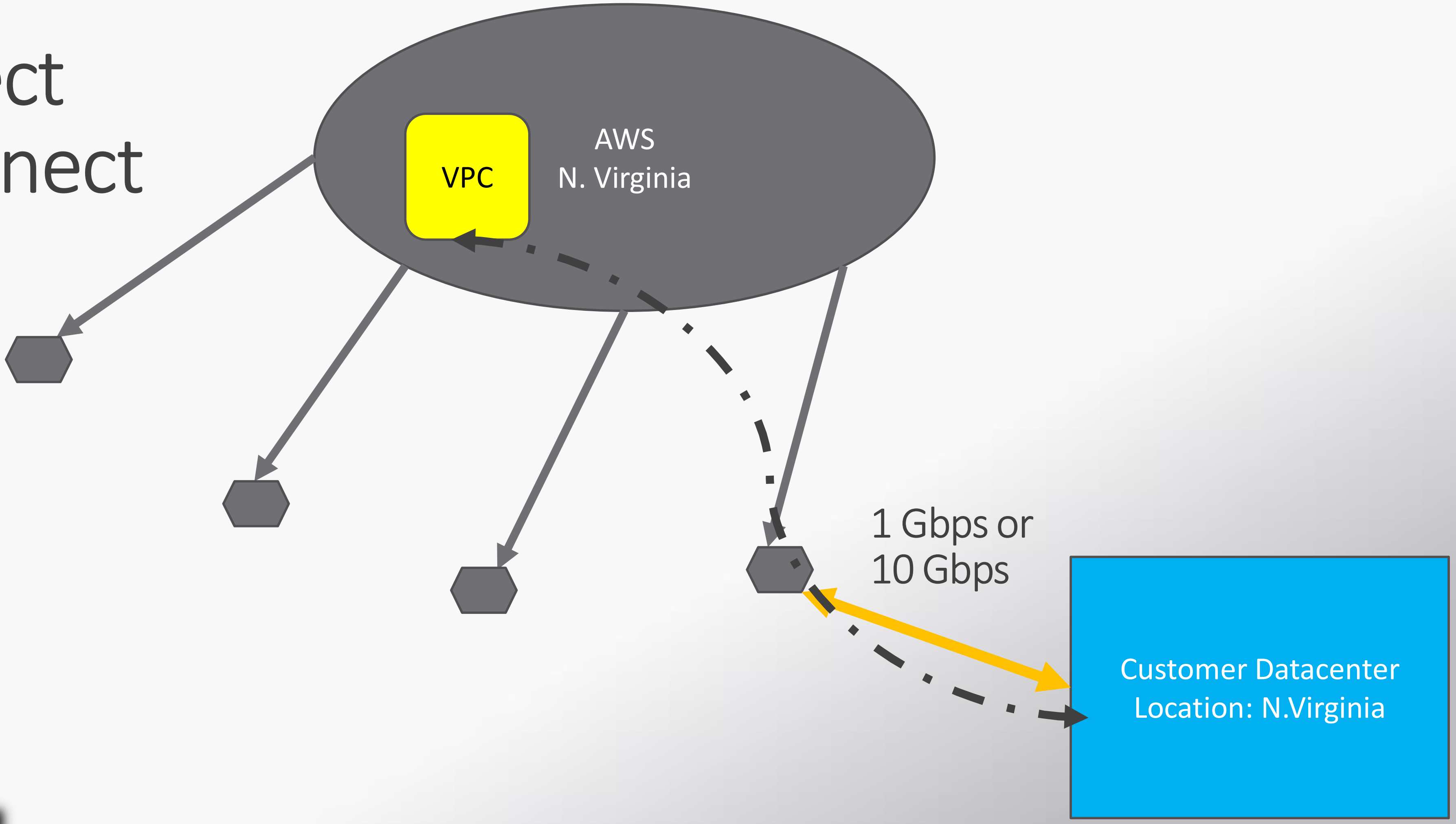
Direct Connect terminology



Direct Connect vs IPSec VPN Connections

- A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet.
- VPN Connections **can be configured in minutes** and are a good solution for immediate needs, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity.
- AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your intranet and Amazon VPC.
- VPN connections are very cheap (**$37.20**/month as of now) as compared to Direct Connect connection as it requires actual hardware and infrastructure and might go in thousands.

Direct Connect



Troubleshooting issue on Direct Connect

1. **Troubleshooting Layer 1 (Physical) Issues**
2. **Troubleshooting Layer 2 (Data Link) Issues**
3. **Troubleshooting Layer 3/4 (Network/Transport) Issues**
4. **Troubleshooting Routing Issues**

Reference Links.

Troubleshooting issue on VPC-Peering

https://aws.amazon.com/premiumsupport/knowledge-center/vpc-peering-connectivity/

Troubleshooting issue on VPN

https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-troubleshooting/

Direct Connect

https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

https://docs.aws.amazon.com/directconnect/latest/UserGuide/Troubleshooting.html