Oracle Cloud VMware Solution – Reference Architecture

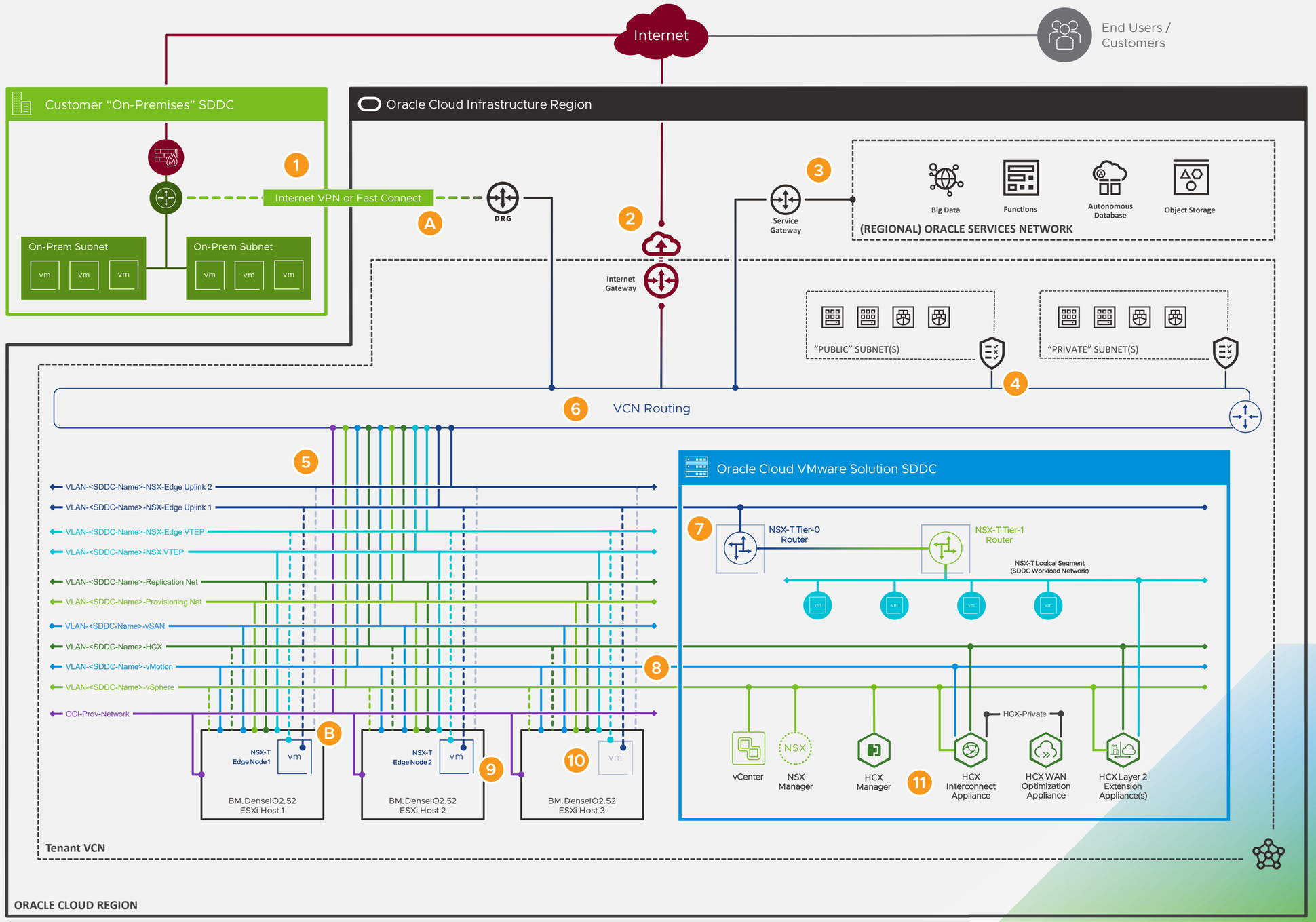
Oracle Cloud Infrastructure and Oracle Cloud VMware Solution SDDC networking reference

This Reference Architecture shows the network topology which underpins Oracle Cloud Infrastructure and its connectivity to Oracle Cloud VMware Solution's infrastructure and workload layers. Also shown is external connectivity from both customer on-premises and mobile users. See cloud.vmware.com/oracle-cloud and www.oracle.com/cloud/compute/vmware/ for more information.

1. External connections over VPN or Fast Connect allow directly routed access without the need for NAT.
2. Internet Gateway allows inbound Internet connections to be terminated on services within Public Subnets or, through NAT onto NSX Edge Uplink VLAN, to workloads within OCVS SDDC.
3. Access to regional OCI services can be routed directly by deploying a Service Gateway into the SDDCs parent VCN.
4. Security lists on Subnets operate like a perimeter firewall for the devices with interfaces within that subnet.
5. Network Security Groups assigned to device interfaces on VLANs operate like a distributed firewall filtering traffic into, out of and between devices within the group.
6. VCN routing is automatic for destinations for which OCI has direct connection/visibility. Where this is not the case, specific Rules need to be added to Route Lists of objects where access is required. This is the case for VCN access to the OCVS SDDC NSX overlay network segments
7. External access from the OCVS SDDC can route directly from its Source address to the VCN. But for Internet egress, it must be NAT'd through the NSX-T Tier-0 router to a VIP on the Uplink VLAN, and from their to a Public IP address through the VCN's Internet Gateway.
8. SDDC Management components are connected to OCI VLAN-backed PortGroups. They are reachable from External Access VIPs assigned to the VLANs, and connect to the VCN routing without traversing the SDDC's NSX-T fabric.
9. Using the "*collapsed cluster*" deployment, the NSX-T Edge Nodes are deployed as VMs on Transport Node hosts. The Edge VMs use separate TEP interfaces to those of their parent hosts. In addition, the Uplink VLANs which will terminate on the Tier-0 Router are also presented to the Edge Node VMs.
10. At deployment time, the HA Edge Nodes are created on Hosts 1 and 2 with anti-affinity rules to keep them on separate hosts. All network connections are also mirrored to the other hosts in the cluster in case an Edge VM is relocated to those hosts.
11. HCX Manager is deployed with each SDDC, but other "fleet" appliances are only deployed when HCX services are activated to/from a peer site by the end customer.

A. VPN Connect relies on the Internet for connectivity but terminates on the DRG, so is shown like this for diagram clarity.

B. Solid connections with a circular end denote direct termination on host VMKernel ports. Dashed host connections denote networks which back guest network PortGroups within vSphere. Networks shown faintly are reserved for future use.



REALIZE WHAT'S POSSIBLE.™