VMware Cloud™ on AWS - Reference Architecture

Horizon 7 on VMware Cloud™ on AWS

This reference architecture illustrates a minimal viable product to start Horizon 7 on VMware Cloud™ on AWS. This reference architecture shows all the components required for a hybrid cloud environment utilizing Horizon Cloud Pod Architecture.

1 **On-Prem connectivity**
IPsec VPN (preferably route-based) or Amazon Direct Connect between on-prem datacenter and VMC on AWS.
- Policy-based VPN: Subnets have to be declared on both sides during the setup. One tunnel is created per subnet. It is recommended to use large subnets.
- Route-based VPN: Subnets are automatically advertised through BGP. BGP configuration is mandatory, no static route can be configured on VMC side.

2 **Firewall rules** for vCenter Access.
- If On-Prem connectivity is configured, allow infrastructure on-prem subnets to access vCenter & ESXi for management.

3 **On-Prem Firewall**
Access from on-prem subnets to VMC Management segment (or at least vCenter and ESXi).
Access from VMC vCenter to on-prem infrastructure services (Active Directory, DNS, Content Library, …)
Access from VMC DMZ to virtual desktops hosted on-premises

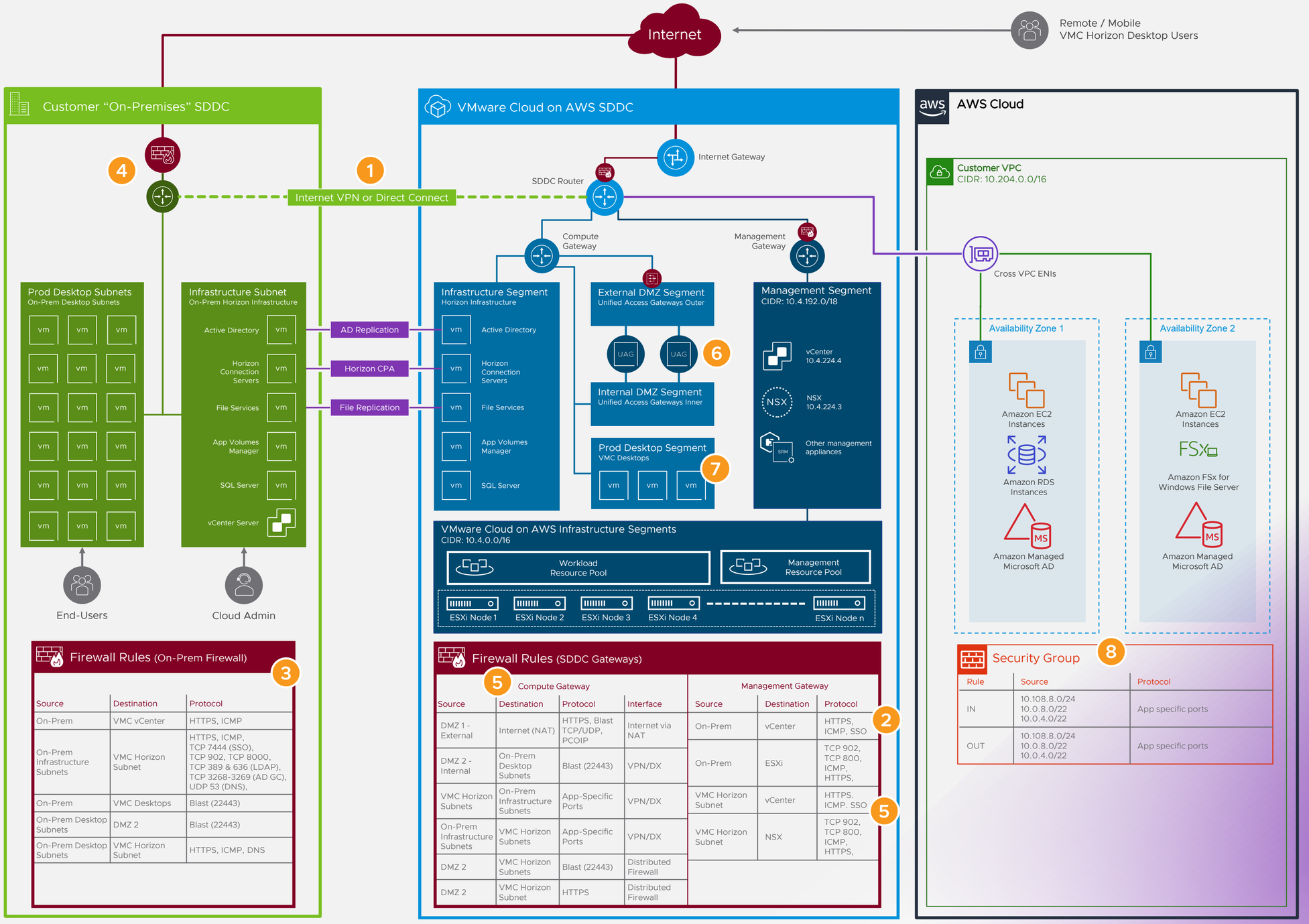
4 **Routed Network Segments**
One Infrastructure segment with privileged access to Management component (vCenter, NSX, …)
Multiple workload segments including:
- Segment for Horizon infrastructure
- Segment for Virtual Desktops or RDSH Servers
- Two DMZ Segments

5 **Firewall rules for Network segments**
- Allow connectivity between Infra & Management
- Allow connectivity between Infra & on-prem infrastructure subnet
- Allow connectivity between workload segment, AWS VPC Subnets and on-prem application subnets
- For Horizon Specific requirements, see the Horizon network ports diagram at https://techzone.vmware.com/resource/network-ports-vmware-horizon-7

6 **DMZ**
Horizon utilizes the Unified Access Gateway for remote access. This appliance can support 1, 2, or 3 network interfaces. A two NIC deployment is recommended.
Two DMZ are needed for a two NIC deployment
- One external-facing DMZ that will be exposed to the Internet via NAT
- One internal-facing DMZ that will connect to Horizon resources in VMC or on-premises

7 **Virtual Desktops and Published Apps**
These are the subnets that Horizon virtual desktops and Published Apps Servers will be deployed into.

8 **VPC connectivity**
This will allow to create hybrid applications leveraging Cloud-Native Services and traditional Virtual Machines
- Allow access from/to VPC subnets and Workload segments in the Compute Gateway and through Security Groups.
- Utilize services like RDS for Horizon and App Volumes databases in place of virtual machines



Firewall Rules (On-Prem Firewall) — 3

Source	Destination	Protocol
On-Prem	VMC vCenter	HTTPS, ICMP
On-Prem Infrastructure Subnets	VMC Horizon Subnet	HTTPS, ICMP, TCP 7444 (SSO), TCP 902, TCP 8000, TCP 389 & 636 (LDAP), TCP 3268-3269 (AD GC), UDP 53 (DNS),
On-Prem	VMC Desktops	Blast (22443)
On-Prem Desktop Subnets	DMZ 2	Blast (22443)
On-Prem Desktop Subnets	VMC Horizon Subnet	HTTPS, ICMP, DNS

Firewall Rules (SDDC Gateways)

5 Compute Gateway				Management Gateway			2
Source	Destination	Protocol	Interface	Source	Destination	Protocol	
DMZ 1 - External	Internet (NAT)	HTTPS, Blast TCP/UDP, PCOIP	Internet via NAT	On-Prem	vCenter	HTTPS, ICMP, SSO	
DMZ 2 - Internal	On-Prem Desktop Subnets	Blast (22443)	VPN/DX	On-Prem	ESXi	TCP 902, TCP 800, ICMP, HTTPS,	
VMC Horizon Subnets	On-Prem Infrastructure Subnets	App-Specific Ports	VPN/DX	VMC Horizon Subnet	vCenter	HTTPS, ICMP, SSO	5
On-Prem Infrastructure Subnets	VMC Horizon Subnets	App-Specific Ports	VPN/DX	VMC Horizon Subnet	NSX	TCP 902, TCP 800, ICMP, HTTPS,	
DMZ 2	VMC Horizon Subnets	Blast (22443)	Distributed Firewall				
DMZ 2	VMC Horizon Subnet	HTTPS	Distributed Firewall				

Security Group — 8

Rule	Source	Protocol
IN	10.108.8.0/24 10.0.8.0/22 10.0.4.0/22	App specific ports
OUT	10.108.8.0/24 10.0.8.0/22 10.0.4.0/22	App specific ports

VMware Cloud™ on AWS