VMware Cloud on AWS - Reference Architecture

Getting Started with VMware Cloud on AWS

This reference architecture provides a generic guidance to start deploying standard hybrid applications on VMware Cloud on AWS that can be accessed by On-Prem end-users.

All networking information depicted here is generic examples and can be customized as per organisation's need.

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 (allowing remote console, vMotion and possibly Hybrid Linked Mode).
- Otherwise, access can be allowed from public Internet but it is highly recommended to limit it to few trusted public IPs (not detailed here)

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, …)

4 **Routed Network Segments**

- One Infrastructure segment with privileged access to Management component (vCenter, NSX, …)
- One or multiple workload segments where all the applications VMs will be deployed.

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

6 **Infrastructure VMs**
Deploying infrastructure VMs inside VMC is recommended to provide reliability and performance to application workloads.
Usual infrastructure components are (but not limited):

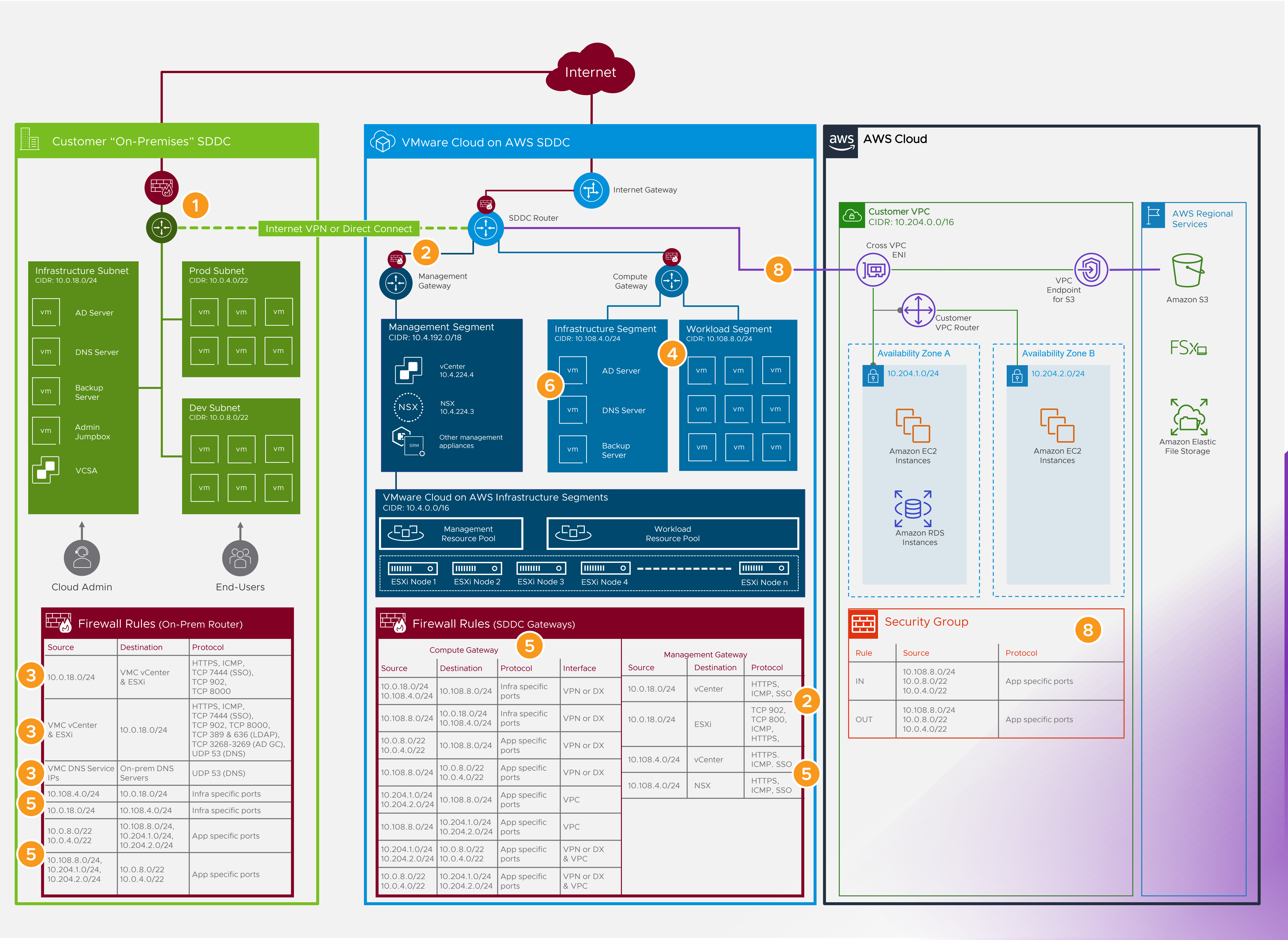
- Active Directory (RODC might be considered)
- DNS Server
- Backup Server

7 **DNS Configuration**

- VMC Compute Gateway should use on-prem DNS servers (applications can resolves enterprise domain)
- vCenter alias to resolve using its private IP (allowing access from on-prem through its alias)

8 **VPC connectivity**
This will allow to create hybrid applications leveraging Amazon Native Services (EC2 & RDS Instances, S3 Buckets, EFS, etc.) and traditional Virtual Machines

- Allow access from/to VPC subnets and Workload segments in the Compute Gateway and through Security Groups.



Firewall Rules (On-Prem Router)

	Source	Destination	Protocol
3	10.0.18.0/24	VMC vCenter & ESXi	HTTPS, ICMP, TCP 7444 (SSO), TCP 902, TCP 8000
3	VMC vCenter & ESXi	10.0.18.0/24	HTTPS, ICMP, TCP 7444 (SSO), TCP 902, TCP 8000, TCP 389 & 636 (LDAP), TCP 3268-3269 (AD GC), UDP 53 (DNS)
3	VMC DNS Service IPs	On-prem DNS Servers	UDP 53 (DNS)
5	10.108.4.0/24	10.0.18.0/24	Infra specific ports
	10.0.18.0/24	10.108.4.0/24	Infra specific ports
5	10.0.8.0/22 10.0.4.0/22	10.108.8.0/24, 10.204.1.0/24, 10.204.2.0/24	App specific ports
	10.108.8.0/24, 10.204.1.0/24, 10.204.2.0/24	10.0.8.0/22 10.0.4.0/22	App specific ports

Firewall Rules (SDDC Gateways)

Compute Gateway 5

Source	Destination	Protocol	Interface
10.0.18.0/24 10.108.4.0/24	10.108.8.0/24	Infra specific ports	VPN or DX
10.108.8.0/24	10.0.18.0/24 10.108.4.0/24	Infra specific ports	VPN or DX
10.0.8.0/22 10.0.4.0/22	10.108.8.0/24	App specific ports	VPN or DX
10.108.8.0/24	10.0.8.0/22 10.0.4.0/22	App specific ports	VPN or DX
10.204.1.0/24 10.204.2.0/24	10.108.8.0/24	App specific ports	VPC
10.108.8.0/24	10.204.1.0/24 10.204.2.0/24	App specific ports	VPC
10.204.1.0/24 10.204.2.0/24	10.0.8.0/22 10.0.4.0/22	App specific ports	VPN or DX & VPC
10.0.8.0/22 10.0.4.0/22	10.204.1.0/24 10.204.2.0/24	App specific ports	VPN or DX & VPC

Management Gateway

Source	Destination	Protocol	
10.0.18.0/24	vCenter	HTTPS, ICMP, SSO	2
10.0.18.0/24	ESXi	TCP 902, TCP 800, ICMP, HTTPS,	
10.108.4.0/24	vCenter	HTTPS. ICMP. SSO	5
10.108.4.0/24	NSX	HTTPS, ICMP, SSO	

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 | aws

VMware Cloud™ on AWS