VMware Cloud™ on AWS - Reference Architecture

Connecting to VMware Cloud on AWS with SSL Client VPN Software

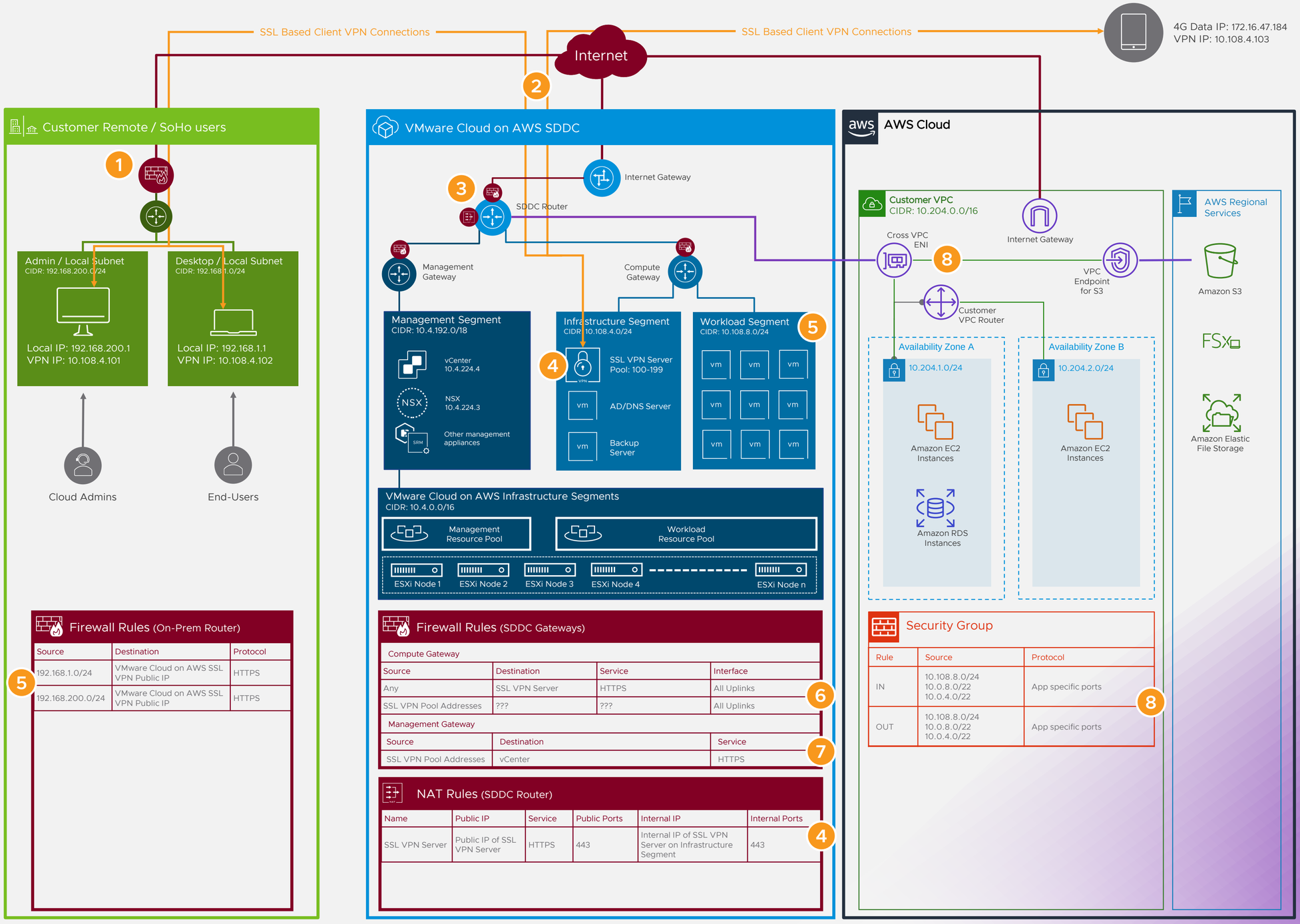
This reference architecture provides guidance to configure standard SSL VPN software on VMware Cloud on AWS that can be used by end-users to access management services and applications running in VMware Cloud on AWS and connected AWS VPCs from anywhere.

Networking depicted here should be considered a generic example and can be customized to meet organizational needs.

1. The solutions depicted here should not be confused with a "Site to Site" (or LAN to LAN) VPN which connects a site router/firewall to the SDDC router using an IPSec VPN to natively connect/route the networks together.
2. Client SSL VPN connectivity is between the user's laptop, workstation or mobile device and an SSL Server appliance VM within VMware Cloud on AWS. Clients could be mobile, home office or, as shown here, small office (without a site to site VPN) locations.
3. To make the SSL Server reachable from the Internet, a "Public" IP address should be provisioned, and a NAT rule created to connect the new public IP address on the SDDC Router to the "private" address of the VPN server on the Infrastructure Segment.
4. Clients are allocated "VPN" IP addresses from a pool configured on the VPN Server. The pool must be from addresses within the same network segment's subnet, as the VPN Server cannot advertise additional "VPN" subnets into the SDDC routing tables.

   If the VPN Client routes all traffic through the VPN tunnel, the SDDC routing tables will direct client traffic to all destinations within and outside the SDDC. If the VPN server allows the client to only route specific traffic over the VPN tunnel (sometimes known as "Split Tunneling"), all required destinations within the SDDC or connected VPC will need to configured (and maintained) on the VPN server so they can be advertised to clients.
5. For VPN clients behind a firewall without a policy which allows "Any" outbound connections, specific rules must be added to allow access to the VPN Server's public IP address.
6. As the source addresses of the VPN clients cannot always be predicted or controlled, the Compute gateway firewall rule should allow "Any" address to reach the VPN server on TCP port 443 (SSL/TLS).

   VPN clients will then be subject to rules based on their VPN pool addresses, so rules will need to be created to allow appropriate access from either the pool, or specific client addresses.
7. If VPN clients require access to the management devices such as vCenter, Management Gateway firewall rules will need to be configured to allow access from either the VPN pool, or specific client addresses.
8. If VPN clients require access to services in, or through, the connected AWS VPC, the VPN pool addresses should be configured for access within the VPC's native Security Group configuration.



VMware Cloud™ on AWS