Active Directory in AWS

Discrete VPCs using IPv6 and IPSec

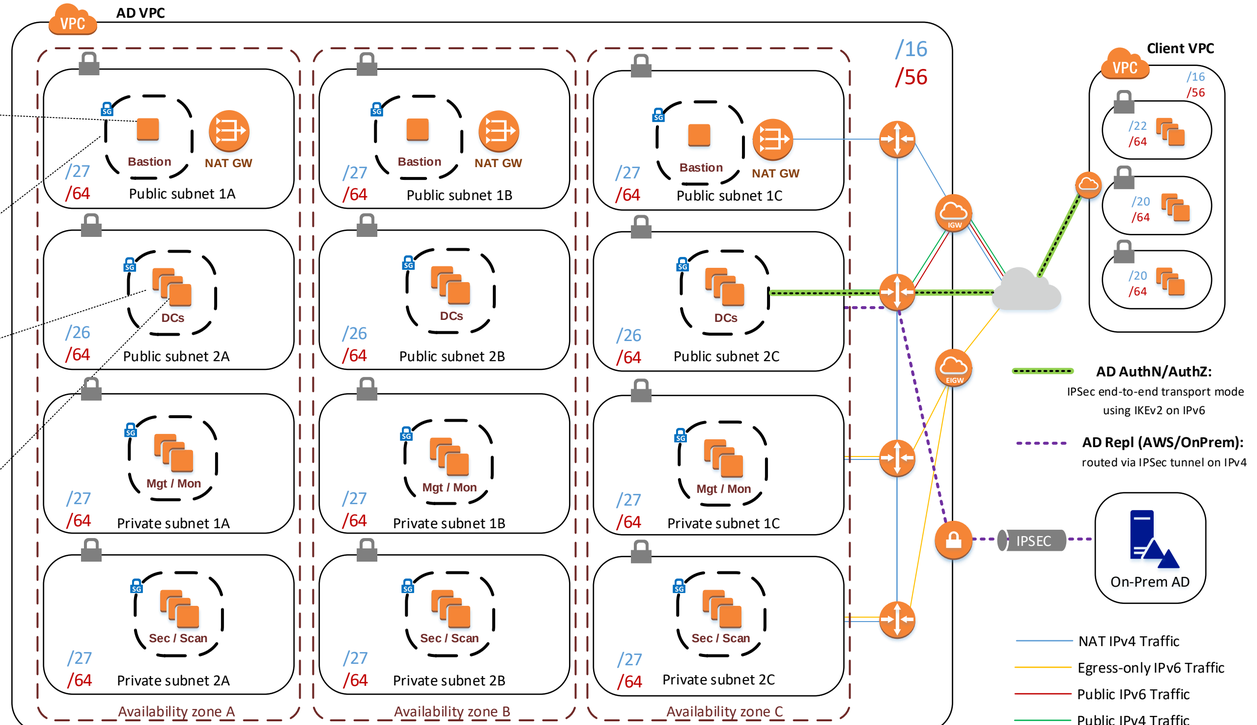
- Domain Controllers in the AD VPC service discrete client VPCs over IPv6
- End-to-end encryption between clients and DCs enforced via IPSec policies, using machine certificates
- The AD VPC and Client VPC(s) may have overlapping private IP space, allowing limitless scaling of connected networks, obviating the need for peering, transit routing, or VPC-to-VPC VPN gateways
- IPv6 cidrs are used to scope security groups, firewalls, and IPSec polices
- Clients can freely manage their own private IP space
- IPv6 cidrs are added to Active Directory Sites and Subnets configuration in order to define an 'AWS site' so that clients in AWS will prefer AWS DCs (for background, see http://aka.ms/Cjpzdd)
- Any windows clients that use IPv6, whether on-prem or in AWS, will prefer AWS domain controllers by way of the IPv6 SRV records
- Intersite Replication between On-Prem and AWS occurs over IPv4 and an IPSec Tunnel using the registered Elastic IPs to define on-prem firewall rules; route table entries ensure that traffic from the AWS DC subnets to campus go through the VPN Gateway
- Additional AD VPCs can be deployed in separate regions, with DC-to-DC communications protected with IPSec transport mode policies, achieving Cross-region redundancy
- Complete reference implementation code (Terraform, Powershell, Vault PKI), as well as packet captures are available for review

Bastion Security Group
allow admin nets & known /32 cidrs:
RDP, WSMAN, SSH

Bastion IPSec Policy
require in/request out, scoped to all nets

Domain Controller Security Group
- allow known /56 cidrs
& onprem nets: AD ports;
- bastion subnets: RDP, WSMAN, SSH

Domain Controller IPSec Policy
require in/request out,
IP-scoped to known /56 cidrs
(exclude on-prem DC subnets),
protocol-scoped to exclude DNS



Public subnet 1A	
0.0.0.0/0	Inet GW
::0/0	Inet GW
2001/56	Local
10/16	Local

Public subnet 1B	
0.0.0.0/0	Inet GW
::0/0	Inet GW
2001/56	Local
10/16	Local

Public subnet 1C	
0.0.0.0/0	Inet GW
::0/0	Inet GW
2001/56	Local
10/16	Local

Public subnet 2A	
0.0.0.0/0	Inet GW
::0/0	Inet GW
2001/56	Local
10/16	Local
On-Prem AD	VPN GW

Public subnet 2B	
0.0.0.0/0	Inet GW
::0/0	Inet GW
2001/56	Local
10/16	Local
On-Prem AD	VPN GW

Public subnet 2C	
0.0.0.0/0	Inet GW
::0/0	Inet GW
2001/56	Local
10/16	Local
On-Prem AD	VPN GW

Private subnet 1A	
0.0.0.0/0	NAT GW A
::0/0	Egress Inet GW
2001/56	Local
10/16	Local

Private subnet 1B	
0.0.0.0/0	NAT GW B
::0/0	Egress Inet GW
2001/56	Local
10/16	Local

Private subnet 1C	
0.0.0.0/0	NAT GW C
::0/0	Egress Inet GW
2001/56	Local
10/16	Local

Private subnet 2A	
0.0.0.0/0	NAT GW A
::0/0	Egress Inet GW
2001/56	Local
10/16	Local

Private subnet 2B	
0.0.0.0/0	NAT GW B
::0/0	Egress Inet GW
2001/56	Local
10/16	Local

Private subnet 2C	
0.0.0.0/0	NAT GW C
::0/0	Egress Inet GW
2001/56	Local
10/16	Local