AWS VPC

A BEST PRACTICES CHECKLIST

Plan your VPC CIDR blocks

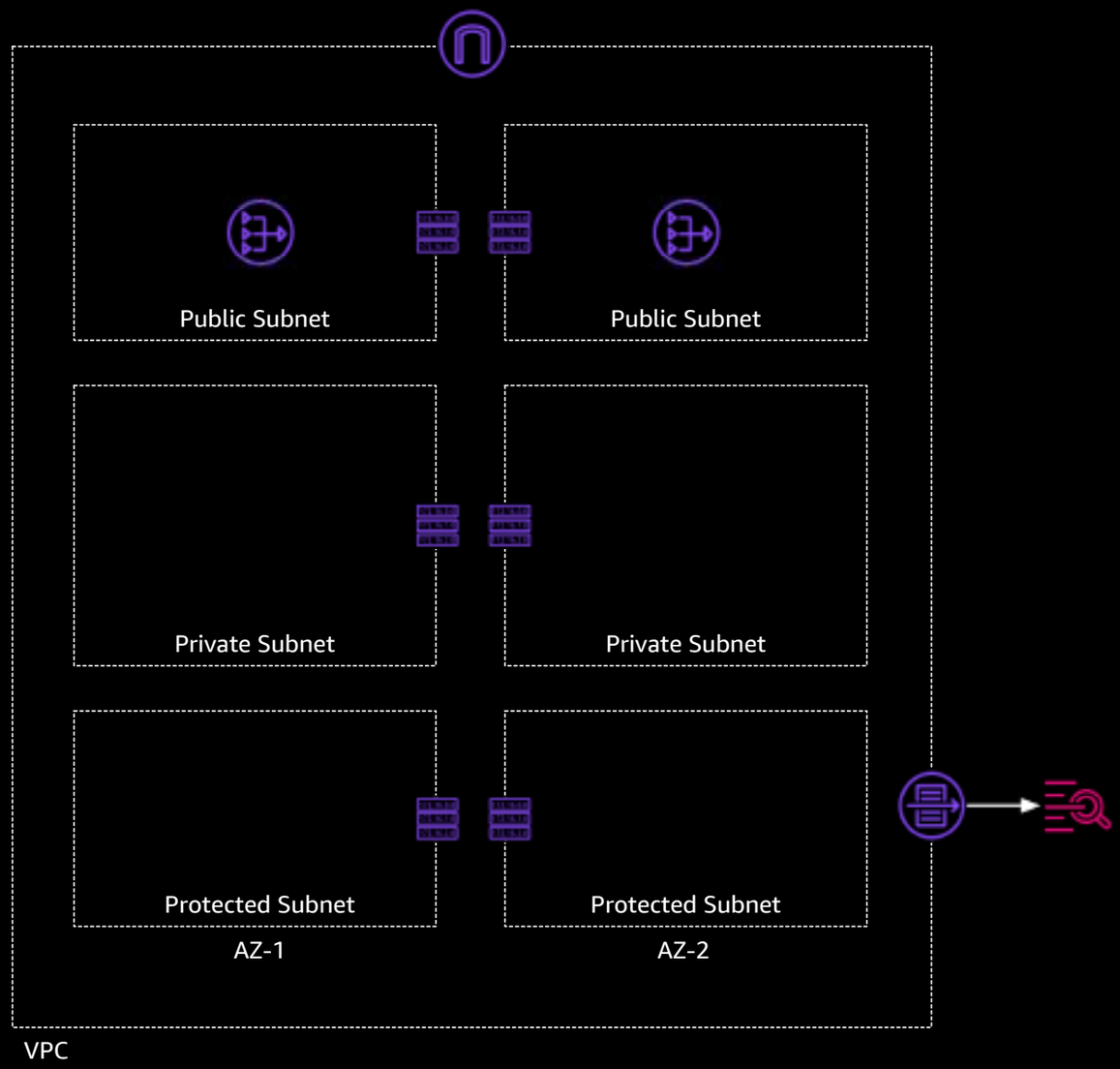
Choose an appropriate CIDR block for your VPC that provides sufficient IP addresses (and room for growth) for your anticipated workloads. Ensure the CIDR block does not overlap with others within your networks or connected networks, such as on-premises data centers or VPCs.

Use subnets and Availability Zones

Divide your VPC into multiple subnets (minimum of 2) spread across different Availability Zones (AZs). This ensures high availability and fault tolerance by allowing your resources to be distributed among separate AZs, reducing the impact of a single point of failure.

Implement network segmentation and security

Implement security groups and network access control lists (ACLs) to enforce strict network access rules. Security groups (required) act as virtual firewalls for your VPC resources, while network ACLs (optional) serve as an additional layer of security for your subnets.



Enable VPC flow logs for monitoring and troubleshooting

Test WAF rules in a staging environment before deploying them to production during a low-activity period to ensure their effectiveness. Use tools like AWS WAF Security Automation or third-party testing services to simulate attacks on your web applications and gauge your WAF configuration. Modify your rules based on the vulnerabilities found during testing.

Use Network Address Translation (NAT) gateways

Deploy NAT gateways in your VPC to enable instances in private subnets to access the internet while preventing inbound internet access. This can help maintain security and prevent unauthorized access to your resources. NAT gateways also provide better performance, availability, and bandwidth management than NAT instances.