AWS Certified Solutions Architect: Associate - 4.0 Amazon Virtual Private Cloud

filename: amazon-acsaa-4-1-virtual_private_cloud
Title: Virtual Private Cloud
Subtitle: AWS Certified Solutions Architect: Associate

4.1 Virtual Private Cloud

- VPC Basics
  - Replaced EC2-Classic
    - Accounts created after Dec 2013 only see VPCs
  - Subnets (Diagram)
    - Classes
      - Public
      - Private
      - VPN-only
        - No internet connectivity beyond VPN
    - Logically separated
    - Each subnet is tied to a single AZ
    - Biggest
      - /16 (65,534)
      - 172.31.0.0/16 is the default
    - Smallest
      - /28 (14)
  - Route Tables
    - Allow traffic to flow between subnets in the VPC
    - Multiple route tables can exist
    - Each subnet must be attached to a route table
    - *Main* route table is used if none specified
  - Internet Gateways (Diagram)
    - Provides internet connection
    - Performs NAT operations
  - DHCP
    - Dynamic Host Configuration Protocol
    - Options can be customized
      - Name servers
      - Domain name
      - Time servers
      - NetBIOS name servers
      - NetBIOS node type
  - Elastic IPs
    - Static IPs
    - Reserved even when an instance is offline
    - Can be reassigned, even between AZs
    - Specific to a region
    - Charged when not in use
  - Elastic Network Interfaces
    - Virtual interfaces than can be reassigned
    - Associated with a subnet
    - Multiple ENIs can be assigned to multi-home an instance
      - Useful for management appliances
  - Endpoints
    - Used for secure communications
    - Allows routing traffic between AWS services without crossing the internet
    - Currently S3 via IPv4 is the only method supported
  - Peering
    - Allows two VPCs to communicate
    - Useful when connecting to another AWS customer's VPC
    - Limited to within the same region
    - No single point of failure
    - Non-transitive (Diagram)
    - Note: CIDR block cannot overlap
  - Security Groups
    - Stateful firewall assigned to an AWS resource
    - All EC2 instances have a Security Group assigned
    - Allows all outbound and denies most inbound by default
    - Details

        - 500 per VPC
        - 50 inbound and 50 outbound rules maximum
        - More than one SG can be assigned to an interface
            - 5 maximum
            - 250 inbound and 250 outbound rules total
        - Rules are applied all at once, not in order
        - Allow rules only, no deny
        - Default SG allows instances to talk to each other
        - New SGs do not allow instances to talk to each other unless you specify it
        - An instance's SG can be changed at any time
- Network Access Control Lists
    - Similar to SGs except assigned at the subnet level
    - Not stateful
    - Default NACL allows all traffic
    - New NACLs deny inbound and outbound traffic
    - Supports allow and deny rules
    - Rules are applied in order
    - Designed as a backup layer of defense
        - Misconfigured SGs
- Network Address Translation
    - Default VPC uses NAT by default
    - Custom VPCs do not, must be configured via an IGW
    - NAT Instance
        - An EC2 instance that performs NAT
        - The "old" way
    - NAT Gateway
        - Managed by Amazon
        - Highly available
        - The "new" way
- Virtual Private Networks
    - Allows creating a hybrid cloud
    - Can connect an on-premises datacenter to a VPC
    - Virtual Private Gateway
        - The VPN endpoint in AWS
    - Customer Gateway
        - The VPN endpoint at the customer location
        - Connection is always initiated by the CGW
        - Usually hardware, but can be software
    - Supports static routing or dynamic (via BGP)
    - Many-to-one is supported
        - Multiple branch offices could all have VPN connections to a single VPG
    - Two tunnels are always created for redundancy