Networking and Security in Cloud Computing

CSYE 6225: Network Structure & Cloud Computing
Northeastern University

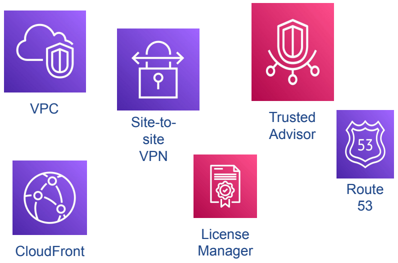
Instructor: Raja Alomari,PhD

M7: Overview

Topics include:

- Virtual Private Cloud (VPC) architecture and configuration.
- AWS CloudFront for content delivery and caching.
- Route 53 DNS management and traffic routing.
- Hybrid networking with Direct Connect and VPN.
- Cloud security best practices and services (WAF, Shield, IAM).

Networking and Security in Cloud Computing



Objectives:

- Understanding cloud networking and content delivery (focus on AWS).
- Core networking services (VPC, CloudFront, Route 53).
- Security measures in cloud environments (IAM, security groups, firewalls).
- Hands-on labs for practical learning.

What is Cloud Networking?

Definition: The integration of networking resources such as firewalls, routers, and switches into the cloud.

- ○ Virtualized resources provided by cloud platforms (AWS, Azure, GCP).
- ○ Key components: VPCs, subnets, gateways, and load balancers.

Traditional Networking vs. Cloud Networking:

- Hardware-based networking (routers, switches) vs. software-defined networks (SDN).
- Cloud eliminates hardware dependencies; everything is virtualized.
- On-demand resource allocation and flexibility.

Amazon VPC Overview

VPC Overview:

- Fully customizable network isolated from other cloud users.
- Control over IP ranges, subnets, route tables, gateways.

Why Use a VPC?

- Ensures data isolation.
- Fine-grained control over traffic.
- Ability to scale based on workload requirements.
- Connectivity options for hybrid cloud environments.

VPC

VPC Components Breakdown

Subnets: Divide VPC into smaller network segments. Public vs. Private subnets.

Route Tables: Control traffic flow within VPC and to external networks.

Internet Gateway (IGW): Connect VPC to the internet.

NAT Gateway: Enable instances in private subnets to access the internet.

Designing a VPC Architecture

Considerations:

- CIDR block selection (IPv4 and IPv6).
- Subnet planning (public/private).
- Multi-AZ (Availability Zones) deployment for redundancy.
- Route table configuration for inter-subnet communication.

Best Practices:

- Use private subnets for backend services (databases, internal APIs).
- Public subnets for web-facing services only.

Understanding CIDR (Classless Inter-Domain Routing)

- What is CIDR?:
  - CIDR is a method for allocating IP addresses more efficiently and routing IP packets.
  - It replaces the old class-based IP addressing system (Class A, B, C).
- CIDR Notation:
  - Written as IP address followed by a slash and prefix length (e.g., 192.168.1.0/24).
  - The number after the slash represents how many bits are used for the network portion of the address.
- Benefits of CIDR:
  - Efficient IP Allocation: Allows networks to use IP addresses more flexibly.
  - Reduces Routing Table Size: Aggregates multiple IP ranges, making routing more efficient.
- Example:
  - 192.168.0.0/16 represents IPs from 192.168.0.0 to 192.168.255.255.
  - 192.168.1.0/24 represents IPs from 192.168.1.0 to 192.168.1.255 (smaller subnet).

CIDR: Example (192.168.0.0/16)

Base IP Address (192.168.0.0): This is the starting IP address of the subnet.

Subnet Mask (/16): The /16 indicates that the first 16 bits of the IP address are used for the network portion, while the remaining bits are used for the host portion.

In binary, the subnet mask is represented as: 11111111.11111111.00000000.00000000

This translates to the decimal subnet mask of **255.255.0.0**

CIDR: Example (192.168.0.0/16)

Network Portion: The first 16 bits (192.168) define the network. All devices on this subnet will share the same network address (192.168).

Host Portion: The remaining 16 bits (0.0) are available for host addresses. This means you can have a total of **2^16 = 65,536** IP addresses in this subnet (from 192.168.0.0 to 192.168.255.255).

In AWS: 5 are reserved addresses (Network Address (192.168.0.0), VPC Router (192.168.0.1), DNS Server (192.168.0.2), Reserved for Future 1 (192.168.0.3), Reserved for Future 2 (192.168.0.4)).

Thus the remaining **2^16 - 5** are available for devices within the VPC.

Advanced VPC Features

VPC Peering: Connect VPCs across regions for cross-application communication.

- Limitations: No transitive peering.

VPC Endpoints: Privately connect to AWS services (e.g., S3, DynamoDB) without an Internet Gateway.

VPC Flow Logs: Monitor and capture network traffic for analysis and troubleshooting.

- Flow logs provide visibility into IP traffic in and out of network interfaces.

Virtual Private Gateway and Direct Connect

- Virtual Private Gateway (VGW):
  - Allows secure communication between your VPC and on-premise network via VPN.
  - Use Case: Hybrid cloud setups.
- AWS Direct Connect:
  - Dedicated high-speed network connection between on-premises and AWS.
  - Use Case: Large-scale data transfers with low latency and high bandwidth.

Direct Connect

Network Address Translation (NAT)

Definition: NAT is AWS service that allows instances in private subnets to initiate outbound traffic to the internet without exposing their private IP addresses.

Types of NAT:

- NAT Gateway: Managed service with high availability.
- NAT Instance: EC2-based, user-managed solution.

NAT Gateway Best Practices:

- Use NAT Gateway for production workloads due to its scalability and ease of use.
- Avoid NAT instance unless cost is a critical factor.

Security in Cloud Networks

Shared Responsibility Model

AWS operates under a shared responsibility model:

- AWS is responsible for the security of the cloud, including the foundational infrastructure such as hardware, software, networking, and facilities.
- Customers, on the other hand, are responsible for the security in the cloud, which involves protecting their data, managing their applications, and configuring services securely.

Shared Responsibility Model: VPC and Encryption

Securing VPC Components

Customers are responsible for securing Virtual Private Cloud (VPC) components, including subnets, internet gateways, NAT gateways, route tables, and network peering connections.

This involves ensuring proper network segmentation and traffic routing to safeguard internal resources.

Encryption

Data at Rest: Customers are responsible for encrypting sensitive data stored in AWS services such as Amazon S3, RDS, EBS, and DynamoDB using AWS Key Management Service (KMS) or other encryption methods.

Data in Transit: Customers must ensure that data transmitted between services, or between on-premises and AWS, is encrypted using protocols like TLS/SSL to prevent eavesdropping.

Shared Responsibility Model: Security Controls

Security Groups: Act as virtual firewalls that control inbound and outbound traffic to AWS resources like EC2 instances. Customers must define appropriate rules to allow only the necessary traffic.

Network Access Control Lists (NACLs): NACLs provide stateless filtering of traffic at the subnet level, offering an additional layer of defense by controlling both inbound and outbound traffic.

IAM (Identity and Access Management): Customers need to implement IAM policies that enforce least privilege access, restricting users and services to only the permissions they need to operate. Role-based access control, multi-factor authentication (MFA), and proper policy versioning are vital for securing access to AWS resources.

Security Groups vs. Network ACLs (NACLs)

Security Groups

- At the instance level.
- Stateful firewall.
- Inbound and outbound rules.
- Allows traffic only from explicitly defined sources.

NACLs

- At the subnet level.
- Stateless firewall.
- Evaluates both inbound and outbound traffic.
- Use for coarse-grained access control across subnets.

Shared Responsibility Model: Patching and Backups

Patch Management

- AWS manages the patching of the underlying infrastructure.
- Customers are responsible for patching the operating systems and applications running on EC2 instances and other managed services like RDS.
- Regular patching helps mitigate vulnerabilities.

Backup and Disaster Recovery (DR)

- Customers must implement proper backup strategies for their data, applications, and services, leveraging tools like AWS Backup or native service snapshots (e.g., EBS, RDS, S3).
- A well-defined disaster recovery plan is critical for minimizing downtime and data loss in the event of failures.

Shared Responsibility Model: Logging and Monitoring

Logging and Monitoring

Customers should configure logging and monitoring tools such as AWS CloudTrail, Amazon CloudWatch, and AWS Config to maintain visibility into API calls, network traffic, and configuration changes. These tools help detect and respond to potential security incidents.

Anomaly and Vulnerability Detection

Setting up AWS GuardDuty and AWS Security Hub provides continuous threat detection, vulnerability assessments, and centralized security management across AWS accounts.

Shared Responsibility Model: Compliance and Automation

Compliance

- AWS offers a wide range of certifications and compliance assurances.
- Customers are responsible for ensuring that their own cloud environments meet the regulatory requirements relevant to their industry, such as GDPR, HIPAA, or PCI-DSS.
- This may involve data classification, audit logging, and managing access to sensitive information.

Automating Security

- Customers can leverage tools such as AWS Lambda, AWS Systems Manager, and AWS Config Rules to automate security processes like patching, resource monitoring, and compliance checks.
- Automation reduces human error and ensures consistent security posture across environments.

Securing Data: At-Rest and in-Transit

Data Encryption in-Transit:

- Use SSL/TLS for encrypting traffic between instances and external services.
- AWS Certificate Manager (ACM) to manage SSL certificates.

Key Management Service (KMS): Encrypt data stored in AWS services (S3, RDS, etc.) using customer-managed keys.

Security at the Edge:

- Enable HTTPS for CloudFront distributions.
- Use AWS Shield to defend against DDoS attacks.

Encryption at Rest:

- Use server-side encryption with KMS or customer-managed keys.
- Secure sensitive data stored in S3, EBS, and RDS.

Key Rotation: Regularly rotate encryption keys to improve security.

Best Practices:

- Enable encryption by default for all storage services.
- Audit encryption policies periodically.

Network Security Best Practices

Segmentation: Organize your VPC into multiple subnets. Use subnets, NACLs and security groups to segment your network.

Least Privilege: Apply IAM policies and security group rules based on the principle of least privilege.

Encryption: Always encrypt data in transit and at rest using AWS KMS and SSL/TLS.

Monitoring: Enable CloudTrail, CloudWatch, and Flow Logs to detect anomalies.

Additional
Cloud Networking and Security Services

Amazon CloudFront: Global CDN

What is CloudFront?:

- Global Content Delivery Network (CDN) to cache and deliver content quickly.
- Use Case: Serving websites, media content, APIs, etc.

CloudFront

Edge Locations:

- Over 400 globally distributed locations to reduce latency.
- Cache static and dynamic content closer to users.

CloudFront Benefits

- Low Latency: Content is cached at edge locations, reducing the distance data needs to travel.
- High Availability: Built-in redundancy across edge locations.

Route 53: DNS in the Cloud

What is Route 53?:

- AWS's scalable DNS service.
- Use Case: Registering domains, routing internet traffic to AWS resources, and performing health checks.

Key Features:

- Domain registration.
- DNS routing policies (latency-based, failover, weighted).
- Global DNS availability.

Route 53

Hybrid Cloud Networking

- What is Hybrid Cloud?:
  a. Integration of on-premises infrastructure with cloud services.
  b. Use Case: Organizations transitioning workloads from on-prem to cloud, or needing secure communication between the two.
- Hybrid Networking Tools:
  a. AWS Direct Connect.
  b. VPN Gateway for site-to-site VPN connections.
  c. VPC Peering for cross-VPC communication.

Site to Site VPN

Direct Connect

VPN Gateway: Site-to-Site VPN

How VPN Gateway Works:

- Secure IPsec tunnels between on-premises network and AWS.
- Redundant VPN tunnels for high availability.
- Use Case: Organizations needing secure, low-latency connections between data centers and AWS.

Site to Site VPN

AWS Direct Connect: Dedicated Network Links

What is Direct Connect?:

- High-speed, private network connection between on-premises and AWS.
- Provides more consistent performance than the internet.

Use Case: Large-scale data transfers or latency-sensitive applications.

Direct Connect Gateway: Connect multiple VPCs across different regions.

Direct Connect

Load Balancing in the Cloud

What is Load Balancing?:

- Distribute traffic across multiple resources (e.g., EC2 instances) to improve performance and availability.

Elastic Load Balancing (ELB):

- Automatically scales based on incoming traffic.
- Types of Load Balancers:
  - Application Load Balancer: Layer 7 (HTTP/HTTPS) load balancing.
  - Network Load Balancer: Layer 4 (TCP) load balancing for extreme performance.
  - Classic Load Balancer: Legacy option supporting both TCP and HTTP/HTTPS.

ELB

Auto Scaling in AWS

What is Auto Scaling?:

- Automatically adjust the number of EC2 instances in response to traffic changes.

Auto Scaling Groups:

- Define scaling policies (e.g., scale out when CPU usage exceeds 70%).
- Launch configurations to define instance types, AMIs, and security groups.

Auto Scaling

Scaling Strategies:

- Reactive Scaling: Adjusts capacity based on real-time metrics (e.g., CPU, memory).
- Predictive Scaling: Uses machine learning to predict future traffic and scale resources proactively.

Amazon Transit Gateway

What is Transit Gateway?:

- A network hub for interconnecting VPCs and on-prem networks.
- Simplifies managing multiple VPCs and VPNs by centralizing routing.

Key Features:

- Supports thousands of VPCs across multiple regions.
- Centralized monitoring and management.
- Cost-effective compared to multiple VPC peerings.

Transit Gateway

VPC Peering: Direct VPC-to-VPC Communication

What is VPC Peering?:

- A direct connection between two VPCs to allow secure communication.
- Limitations: No transitive peering; traffic cannot pass through more than two VPCs.

Use Case: Connect VPCs owned by different accounts or regions for cross-application communication.

Monitoring and Auditing Cloud Networks

AWS CloudWatch:

- Monitor network performance, traffic metrics, and resource usage.
- Set up custom alarms and dashboards.

VPC Flow Logs:

- Capture and analyze IP traffic to and from network interfaces.
- Use flow logs for troubleshooting and forensic analysis.

CloudWatch

CloudTrail: Network Activity Auditing

What is AWS CloudTrail?:

- Tracks API calls made to AWS resources (e.g., EC2, VPC, S3).
- Use Case: Security auditing and compliance.

Best Practices:

- Enable CloudTrail across all AWS regions.
- Set up centralized logging for easy access to logs.

CloudTrail

AWS Shield, AWS WAF

AWS Shield: DDoS protection for applications hosted on AWS. Two tiers: Shield Standard and Shield Advanced.

Shield

WAF

AWS WAF (Web Application Firewall):

- Protects web applications from SQL injection, cross-site scripting (XSS), and other attacks.
- Custom rule sets to filter traffic based on IP, headers, or query strings.

AWS Inspector

What is AWS Inspector?

- Overview: A security assessment service that helps improve the security and compliance of applications deployed on AWS.
- Purpose: Automatically assesses applications for vulnerabilities or deviations from best practices.

Key Features

- Automated Security Assessments: Scans for security vulnerabilities in applications.
- Built-in Rules Packages: Includes predefined rules based on common compliance standards (e.g., CIS, PCI DSS).
- Detailed Reports: Provides detailed findings and remediation guidance to improve security posture.
- Integration with CI/CD: Works seamlessly with AWS CodePipeline and other CI/CD tools for continuous security assessments.

Hands-on

Objectives:

- ○ Create VPC, public and private subnets.
- ○ Understand IPv4 CIDR format.
- ○ Go over Autoscaling, ELB, Route53, CDN, CloudWatch, CloudTrail, KMS, CloudFront, AWS Shield, GuardDuty, TrustedAdvisor, Inspector.

Module 7 Conclusion

- Cloud networking simplifies infrastructure management with scalable, secure, and cost-effective solutions.
- Amazon VPC and CloudFront enable efficient global content delivery and secure cloud environments.
- Hybrid and multi-region architectures enhance performance, disaster recovery, and availability.
- Security best practices like encryption, monitoring, and IAM are critical for protecting cloud networks.