Networking in the Cloud Era

TEKsystems Global Services

WORKFORCE DEVELOPMENT

COURSE STRUCTURE

Day 1: Networking Fundamentals I

Day 2: Networking Fundamentals II

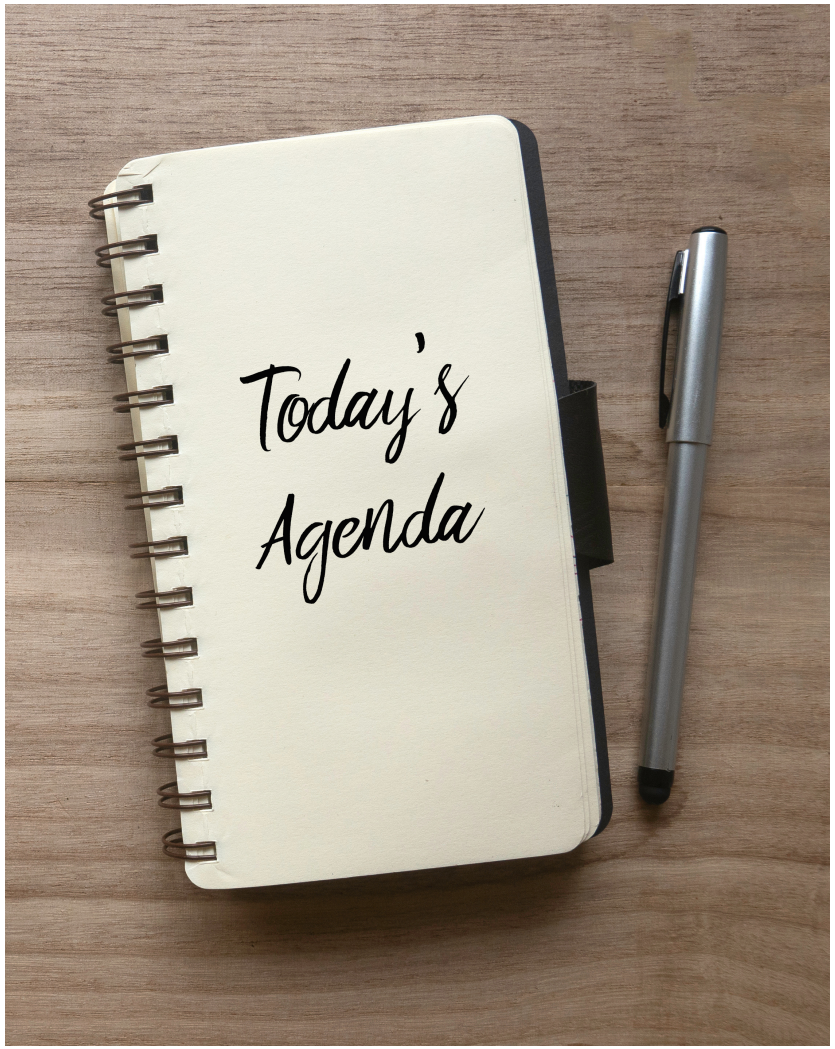
Day 3: Networking in the Cloud Era

Day 4: Cloud Network Services & Connectivity

Day 5: Availability & Troubleshooting in the Cloud

AGENDA FOR DAY 3

1. Networking in the Cloud Era
2. Security & Connectivity
3. Infrastructure as Code (IaC) Concepts



NETWORKING IN THE CLOUD ERA

CLOUD TECHNOLOGIES

- The cloud is on-demand access to computing resources (servers, storage, databases, networking, software) over the Internet.
- Instead of owning physical infrastructure, organizations rent resources from cloud providers.
- Examples of the top 3 cloud providers

CLOUD SERVICES MODELS

- IaaS (Infrastructure as a Service): Virtual servers and storage
- PaaS (Platform as a Service): Tools for app development
- SaaS (Software as a Service): Ready-to-use apps

WHY COMPANIES ARE MOVING TO THE CLOUD

- Cost Efficiency – Pay for what you use; no need to buy hardware.
- Scalability – Easily handle peak demand and scale down when idle.
- Accessibility – Work from anywhere with an internet connection.
- Innovation Speed – Faster deployment of new features and services.
- Resilience & Security – Built-in backups, redundancy, and global security standards.

REAL WORLD USE CASES

- Netflix: Uses AWS for global content delivery and scaling. Precursor of Chaos Engineering
- Airbnb: Runs its platform on cloud infrastructure.
- Banks & Insurance Companies: Using private/hybrid cloud for secure data processing.

MAPPING TRADITIONAL TO AWS NETWORKING

On-Prem Concept	AWS Equivalent
VLAN / Switch	Subnet
Router	Route Table + Gateways
Firewall	Security Group / Network ACL
IP Address Mgmt	VPC CIDR Block
DHCP Server	AWS DHCP Options Set
Physical Cable	AWS Virtual Network Fabric

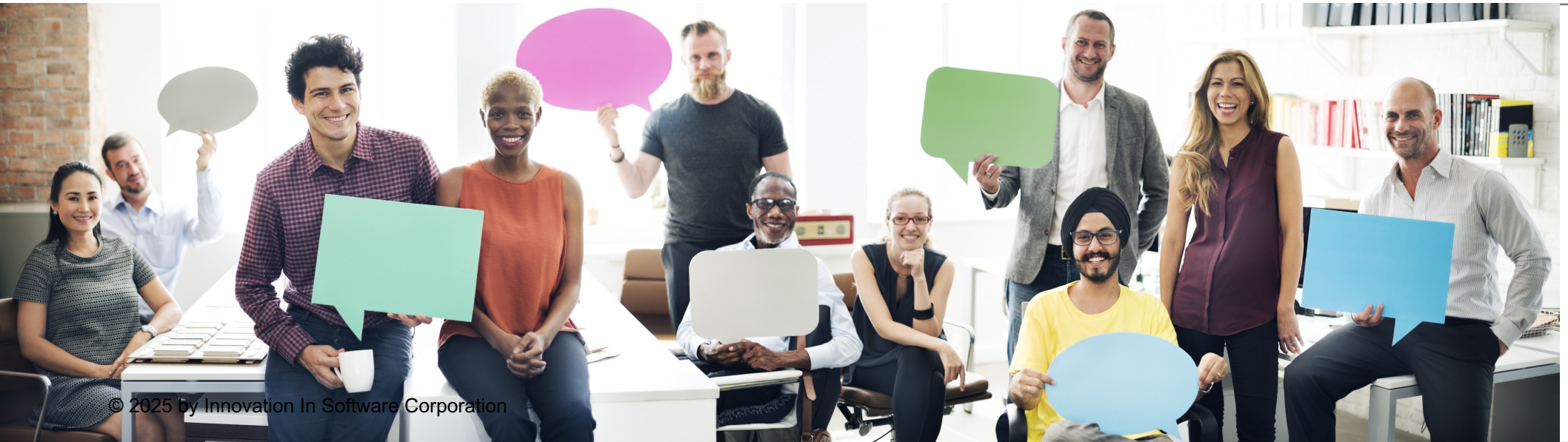
AWS GLOBAL NETWORK STRUCTURE

- VPC CIDR Block: Defines IP range (e.g., 10.0.0.0/16)
- Subnets: Divide your network into public and private zones, 1 AZ per subnet
- Route Tables: Direct traffic between subnets or to external destinations
- Gateways: Enable communication to the internet or other networks
- Elastic Network Interfaces (ENIs): Virtual NICs attached to resource

POP QUIZ:

What is a key reason organizations move to the cloud for cost efficiency?

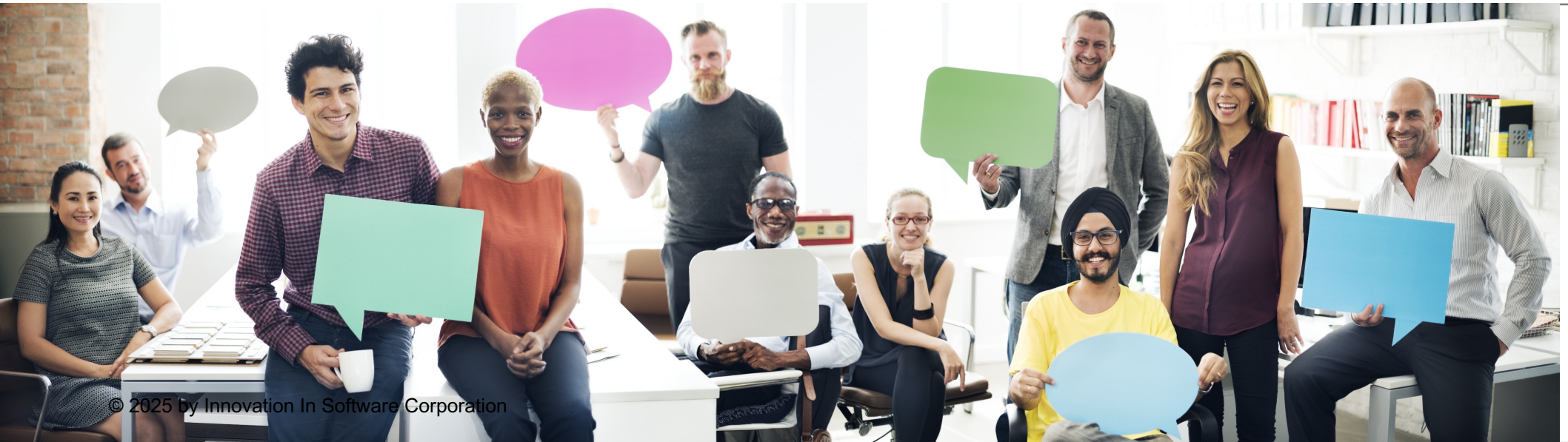
A. They pay for hardware in advance
B. They pay only for what they use
C. They have fixed monthly costs
D. They must maintain servers on-site



POP QUIZ:

What is a key reason organizations move to the cloud for cost efficiency?

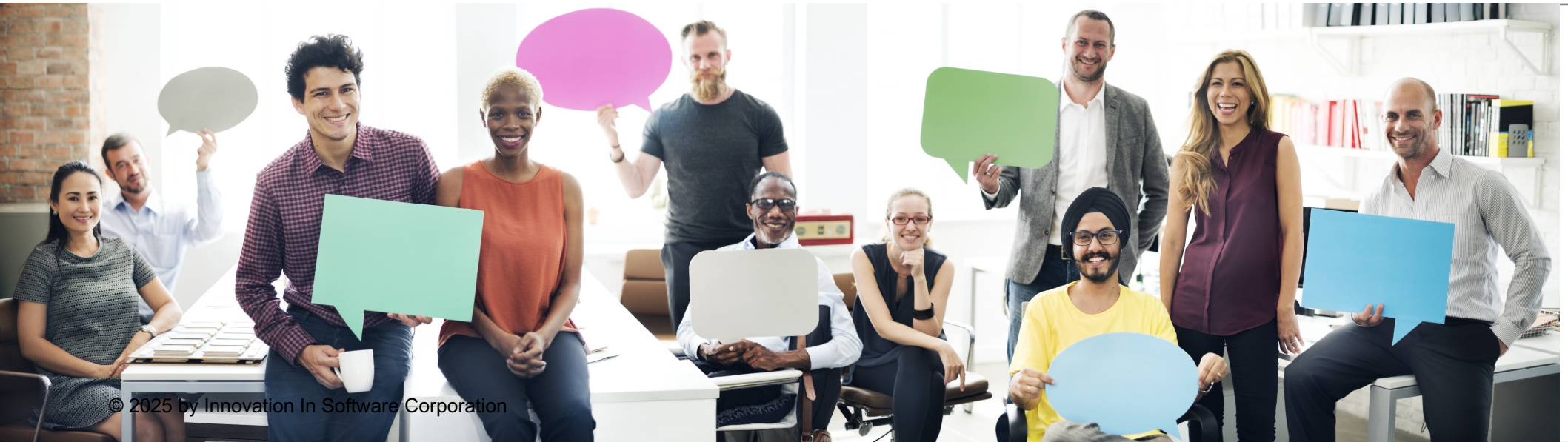
A. They pay for hardware in advance
B. They pay only for what they use
C. They have fixed monthly costs
D. They must maintain servers on-site



POP QUIZ:

Which cloud model allows developers to build and deploy applications without managing servers?

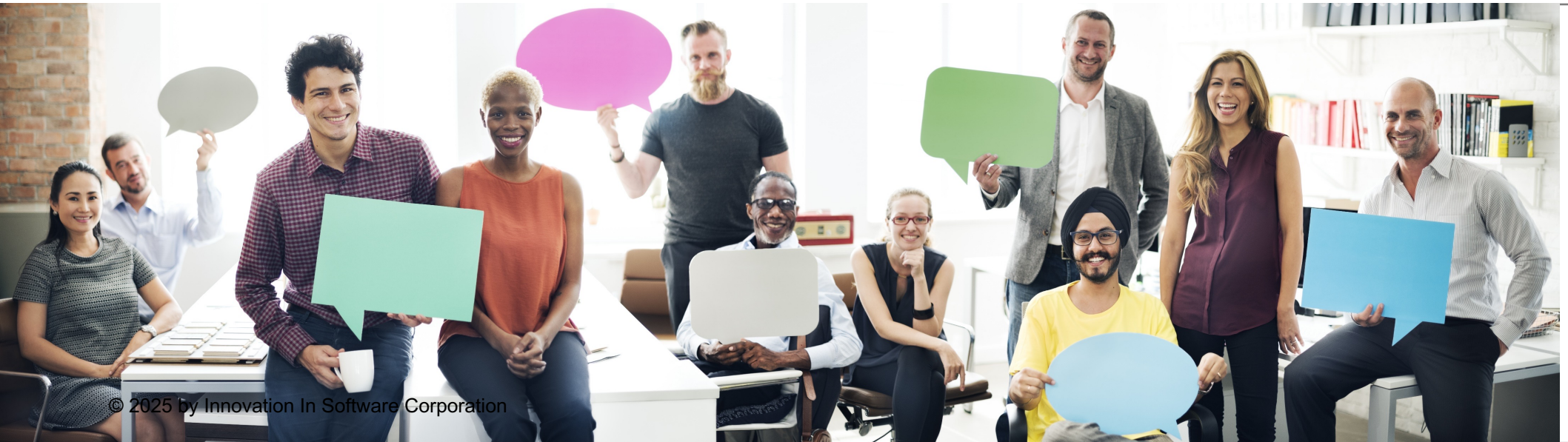
A. IaaS
B. PaaS
C. SaaS
D. DaaS



POP QUIZ:

Which cloud model allows developers to build and deploy applications without managing servers?

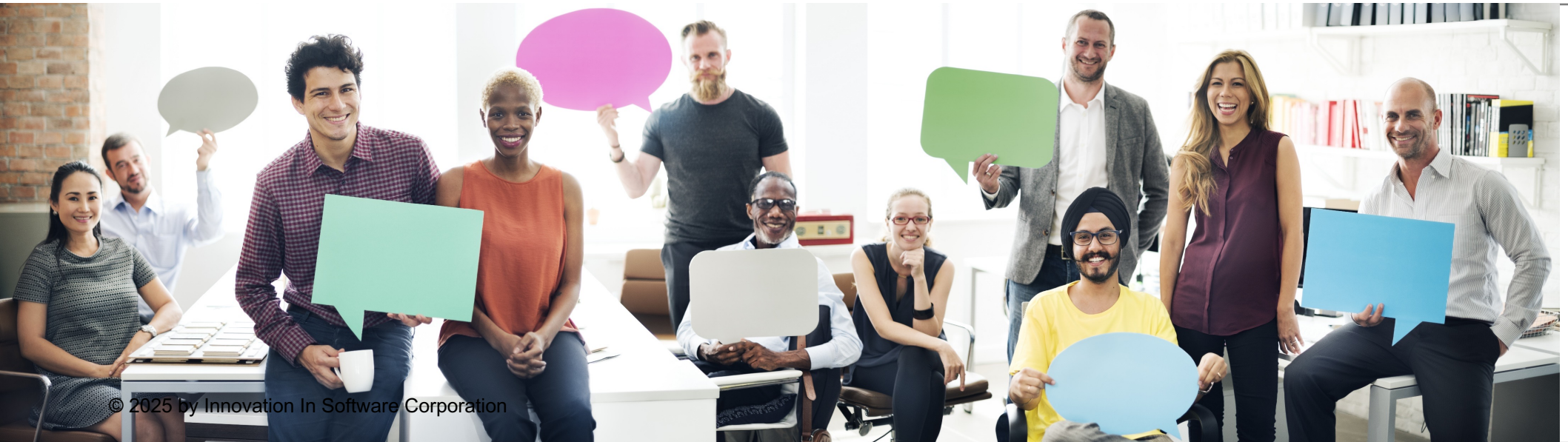
A. IaaS
B. PaaS
C. SaaS
D. DaaS



POP QUIZ:

Which model gives the customer the most control over virtual machines and networking?

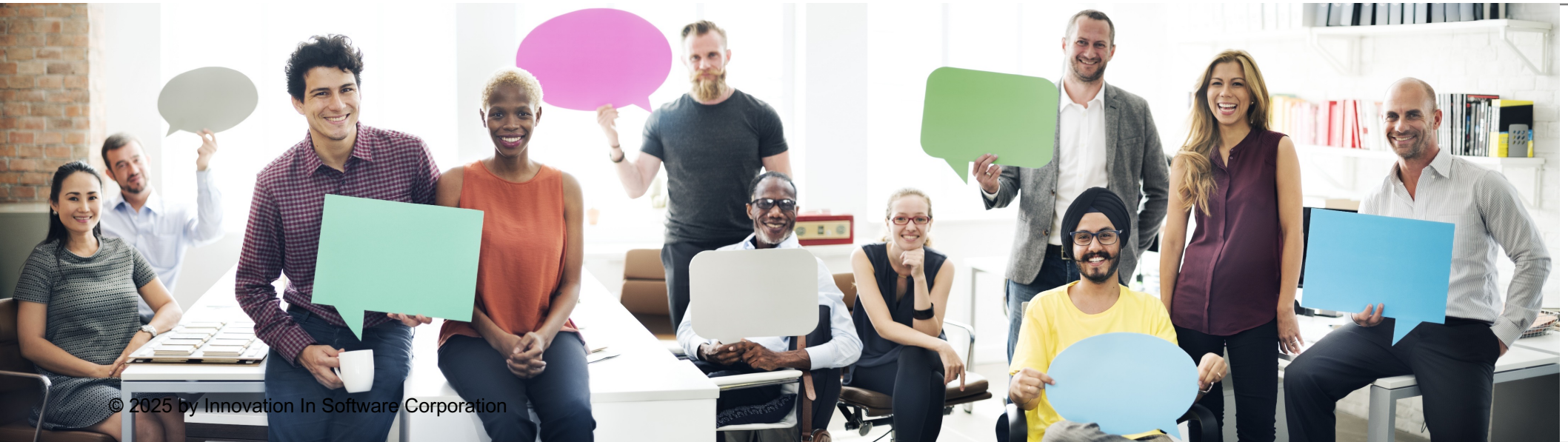
A. SaaS
B. PaaS
C. IaaS
D. FaaS



POP QUIZ:

Which model gives the customer the most control over virtual machines and networking?

A. SaaS
B. PaaS
C. IaaS
D. FaaS



LAB 00: AWS EC2 INTRODUCTION

- Goal: Launch and manage AWS EC2 instances.
- Steps:
  - Create AWS account and configure billing alerts.
  - Launch EC2 instance with proper security groups.
  - Connect via SSH and configure basic services.
  - Understand AWS pricing and cost optimization.

SECURITY & CONNECTIVITY

PUBLIC VS PRIVATE SUBNETS

- Similar to physical network, we will use public and private subnets for security

Subnet Type	Typical Resources
Public	Web servers, bastions
Private	Databases, internal services

ROUTE TABLES AND ROUTING

- Local Route: Enables intra-VPC communication between subnets within the same VPC.

- Default Route (0.0.0.0/0): Directs internet-bound traffic to an Internet Gateway (IGW) for public subnets or to a NAT Gateway (NAT GW) for private subnets.

- Custom Routes:
- Used for advanced network connectivity, such as
  - VPC Peering connections
  - Transit Gateway attachments (covered in later modules)

- Subnet Association:
- Each subnet must be explicitly associated with a route table to define its traffic flow.

SECURITY GROUPS (SGS)

- Stateful: Return traffic is automatically allowed when the inbound rule permits it.
- Attachment: Applied directly to Elastic Network Interfaces (ENIs) or EC2 instances.
- Rule Type: Allow rules only — all other traffic is implicitly denied.
- Example:
  - Allow HTTP (port 80) from anywhere
  - Allow SSH (port 22) only from an admin IP

NETWORK ACLS (NACLS)

- Stateless:
  - Both inbound and outbound rules must be explicitly defined — return traffic is not automatically allowed.
- Scope:
  - Applied at the subnet level, affecting all resources within that subnet.
- Rule Evaluation:
  - Processed in ascending order based on rule number (lowest number takes priority).
- Purpose:
  - Provides an additional layer of security beyond Security Groups.

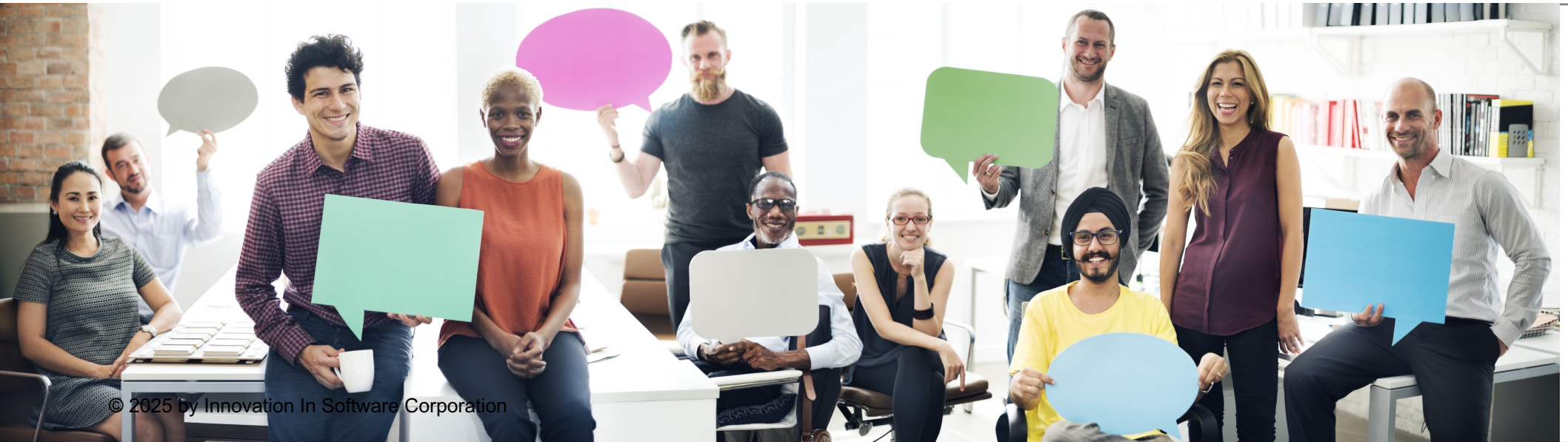
SG VS NACL COMPARISON

Feature	Security Group
Scope	Instance (ENI)
Stateful?	✅
Default	Deny all inbound / allow all outbound
Rule Type	Allow only
Use Case	App tier filtering

POP QUIZ:

What is a public subnet in AWS typically used for?

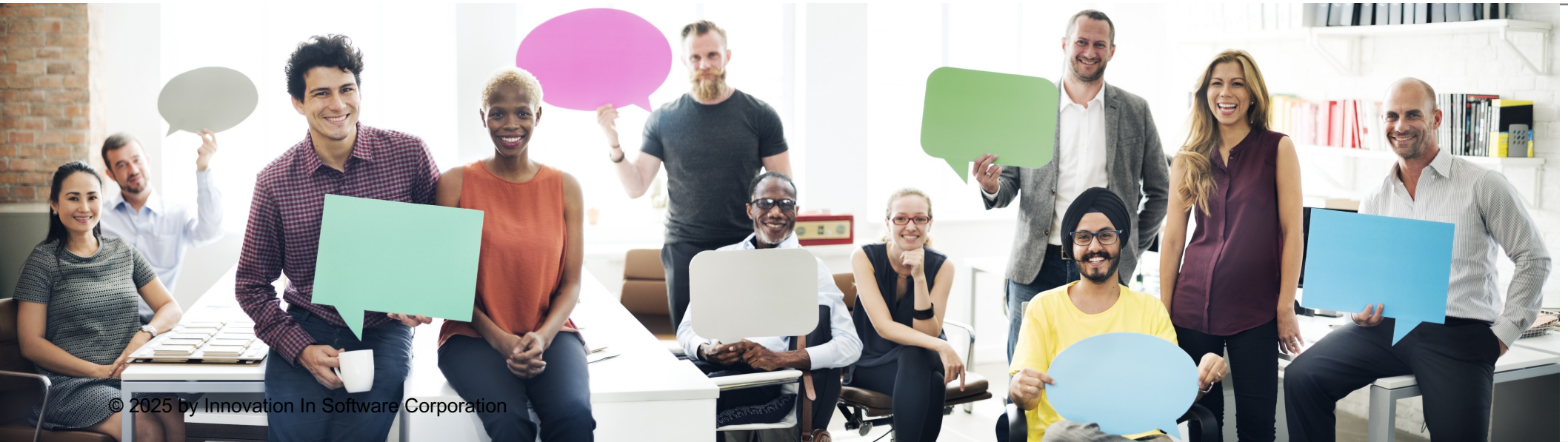
A. Hosting backend databases
B. Hosting internet-facing services
C. Internal-only services
D. Private DNS management



POP QUIZ:

What is a public subnet in AWS typically used for?

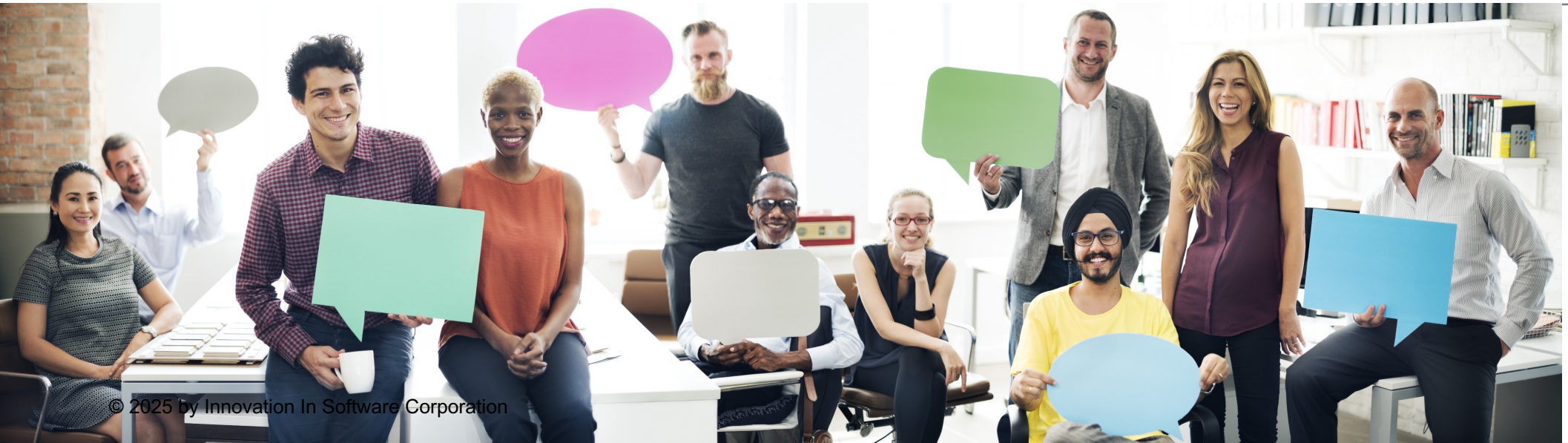
A. Hosting backend databases
B. Hosting internet-facing services
C. Internal-only services
D. Private DNS management



POP QUIZ:

What type of firewall are AWS Security Groups?

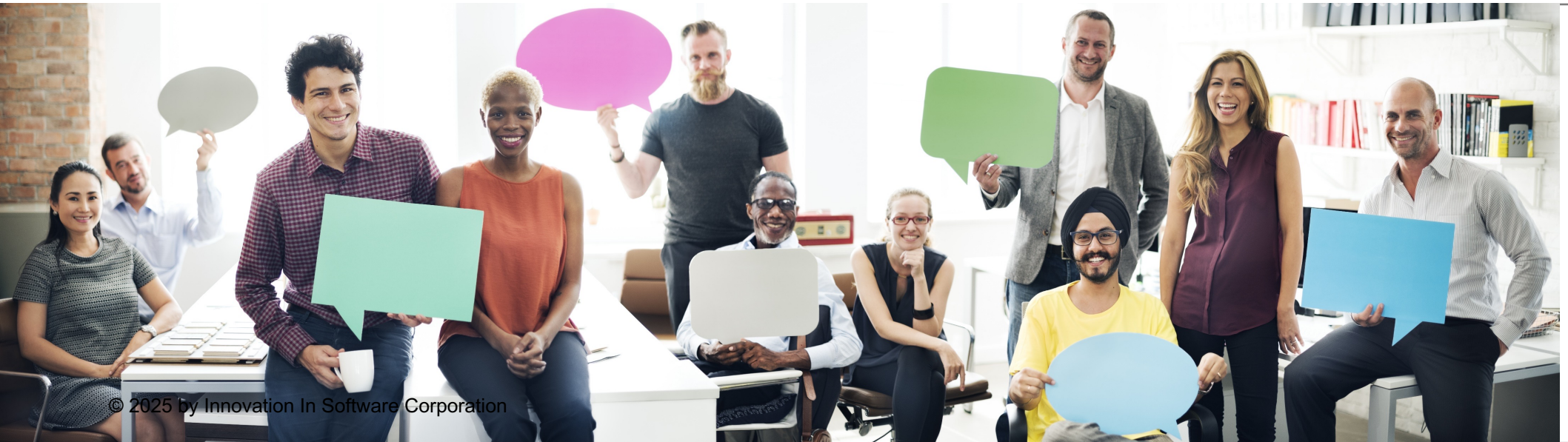
A. Stateless
B. Stateful
C. Dynamic
D. Packet filter only



POP QUIZ:

What type of firewall are AWS Security Groups?

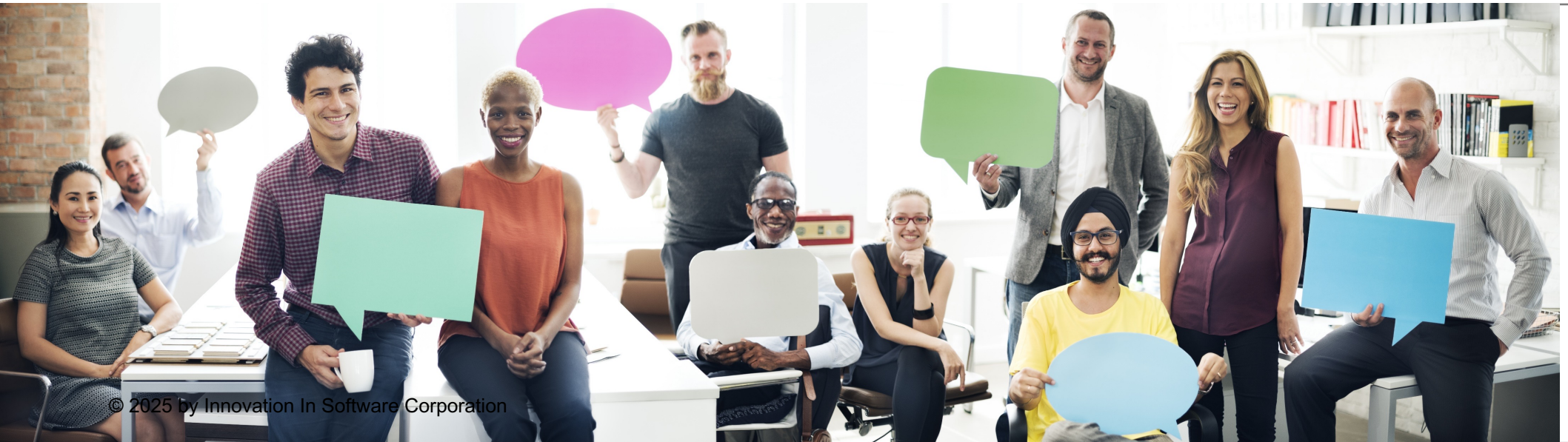
A. Stateless
B. Stateful
C. Dynamic
D. Packet filter only



POP QUIZ:

How are NACLs different from Security Groups?

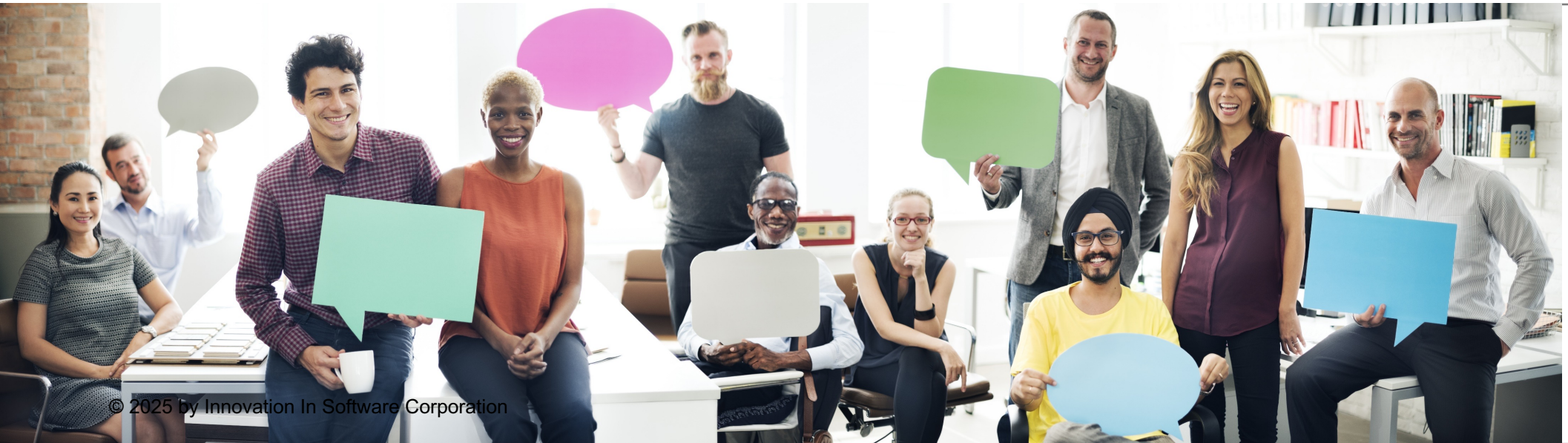
A. NACLs are stateful
B. NACLs are stateless and evaluated per subnet
C. NACLs apply only to EC2 instances
D. NACLs automatically allow all traffic



POP QUIZ:

How are NACLs different from Security Groups?

A. NACLs are stateful
B. NACLs are stateless and evaluated per subnet
C. NACLs apply only to EC2 instances
D. NACLs automatically allow all traffic



LAB 1 OVERVIEW: BUILD YOUR FIRST VPC

- Goal: Create secure cloud network infrastructure.
- Steps:
  - Design VPC with public and private subnets.
  - Configure Internet Gateway and NAT Gateway.
  - Set up route tables for traffic flow.
  - Launch instances in appropriate subnets.

LAB 02: AWS SECURITY GROUPS

- Goal: Implement instance-level firewall rules.
- Steps:
  - Create security groups with specific rules.
  - Configure inbound and outbound traffic policies.
  - Test connectivity between security group members.
  - Apply least-privilege security principles.

LAB 03: AWS NETWORK ACLS

- Goal: Configure subnet-level network filtering.
- Steps:
  - Create custom Network ACL rules.
  - Compare stateful vs stateless filtering.
  - Test NACL rule precedence and numbering.
  - Troubleshoot connectivity with dual security layers.

INFRASTRUCTURE AS CODE (IAC) CONCEPTS

WHY IAC MATTERS

- Traditional Approach:

Manual configuration is slow, error-prone, and leads to inconsistencies between environments.

- Infrastructure as Code (IaC): Infrastructure is defined, managed, and provisioned through code instead of manual processes.

- Key Benefits:
  - Version Control: Track and manage changes like application code.
  - Repeatability: Easily reproduce environments across stages.
  - Automation: Faster, consistent deployments with reduced human error.

TOOLS TO ENABLE IAC

- Multiple tools will allow us to achieve IaC

Tool	Focus
Terraform	Multi-cloud
CloudFormation	AWS native
Ansible	Configuration
Chef/Puppet	OS-level mgmt