# Practical : 10

## Overview

This guide demonstrates IDS/IPS deployment in cloud platforms such as Google Cloud, AWS, or Azure, focusing on protecting virtual networks, monitoring intra-cloud traffic, and responding to threats against cloud resources.

### Step 1: Selecting Cloud IDS/IPS Solutions

- Choose your cloud provider's native IDS/IPS (e.g., Google Cloud IDS, AWS GuardDuty, Azure Network Security Group with integrations) or third-party IDS/IPS appliances available on their marketplace.[1][2]
- For advanced use cases, consider third-party images like Suricata, Snort, or Palo Alto cloud firewalls, which can be deployed onto VMs in the cloud.

### Step 2: Deploy IDS/IPS Endpoints

- Use the cloud provider's management console or CLI tools to deploy IDS/IPS endpoints in regions where you want monitoring.~~[3]~~[1]
- For Google Cloud:
  - Go to Cloud IDS > Create IDS Endpoint.
  - Choose the region and associate the endpoint with your VPC or subnet.
  - Configure throughput (ensure one IDS endpoint per 5Gbps for balanced performance).

### Step 3: Configure Traffic Mirroring/Inspection

- Enable packet mirroring or traffic capturing so IDS/IPS sensors receive both ingress and egress traffic.[1]
- In Google Cloud, use packet mirroring policy to allow mirrored traffic to IDS endpoint.
- In AWS, use VPC Traffic Mirroring to route relevant flows to a monitoring instance with IDS/IPS.
- For virtual appliances, configure them in the path of network flows—either as in-line (IPS) or passive (IDS)—with appropriate routing/firewall rules.[2]

### Step 4: Set Up Detection Policies and Alerting

- Define signature sets for relevant threats: tune rules for applications and services in use, minimizing false positives.[1]
- In cloud-native IDS, set desired alert severity (informational, warning, critical).
- Enable automated alert forwarding to SIEM, email, or other incident management systems.

### Step 5: Firewall Policy Integration

- Integrate firewall rules for network segmentation:
  - Permit required traffic and enforce Layer 7 inspection via the IDS/IPS engine.[3]
  - Example: In Google Cloud's firewall policy, set up rules for inspection before traffic reaches VM endpoints.

### Step 6: Test Protection and Fine-tune

- Simulate typical attack scenarios (port scan, web vulnerability scan) against VMs or services in protected subnets.
- Check the IDS/IPS dashboards and verify accurate detection.
- Review logs and tune signatures, thresholds, and alerting policies for optimal coverage.[1]

## Best Practices

- Deploy IDS/IPS sensors in every region/subnet needing protection.[1]
- Encrypt and securely manage IDS/IPS configurations and credentials.[4]
- Regularly update rules and security profiles to address new threats.
- Integrate IDS/IPS with centralized security management (SIEM, Security Operations Center).

## Reference Material

- Google Cloud: Best practices for Cloud IDS, Set up intrusion prevention service.[3][1]
- Check Point: Cloud IPS features and integration guidance.[2]

Use these steps and best practices when presenting your practical on cloud-based IDS/IPS deployment for protecting virtual networks.