**1. Resource Monitoring Techniques**

Resource monitoring involves tracking the performance and usage of system components like CPU, memory, disk, and network. Techniques include:

**a. Agent-based Monitoring:**

* Tools like **Nagios**, **Zabbix**, and **Datadog** install agents on servers to collect metrics.
* Agents provide detailed insights into system performance.

**b. Agentless Monitoring:**

* Uses protocols like SNMP, WMI, or SSH.
* Tools: **SolarWinds**, **PRTG Network Monitor**.

**c. Cloud-native Monitoring:**

* Built-in tools for cloud platforms:

**AWS CloudWatch**

**Azure Monitor**

**Google Cloud Operations Suite (formerly Stackdriver)**

**d. Log Monitoring:**

* Collects and analyzes logs.
* Tools: **ELK Stack (Elasticsearch, Logstash, Kibana)**, **Splunk**, **Graylog**.

**e. Performance Profiling Tools:**

* For detailed application-level monitoring.
* Examples: **New Relic**, **AppDynamics**, **Dynatrace**.

**2. How to Access Compute (Windows and Linux) from Internet: Tools and Security**

**a. Access Methods:**

| **OS** | **Access Method** | **Tools** |
| --- | --- | --- |
| Windows | Remote Desktop Protocol | RDP (mstsc), AnyDesk |
| Linux | Secure Shell (SSH) | PuTTY, OpenSSH, MobaXterm |

**b. Security Practices:**

1. **Firewall Rules:**

Allow access only from specific IP addresses.

Use network security groups (NSGs) or firewall settings in cloud platforms.

1. **VPN or Bastion Hosts:**
   * Instead of direct access, connect through a secure VPN or a hardened jump server (bastion host).
2. **Multi-Factor Authentication (MFA):**
   * Enforce MFA for all remote access.
3. **Key-based Authentication for SSH:**
   * Use public/private key pairs instead of passwords.
4. **Remote Desktop Gateway:**
   * Secure RDP traffic through a gateway service.
5. **Access Logs and Monitoring:**
   * Enable logging of remote access and set up alerts for suspicious activity.

**3. Encryption Technologies and Methods**

Encryption ensures data confidentiality and integrity. Common types and methods include:

**a. Encryption Types:**

* **At Rest:** Data stored on disk (e.g., disk encryption using BitLocker or LUKS).
* **In Transit:** Data moving across the network (e.g., TLS, HTTPS).
* **End-to-End:** Ensures only communicating users can read the messages (e.g., Signal, WhatsApp).

**b. Encryption Methods:**

| **Method** | **Description** | **Examples** |
| --- | --- | --- |
| Symmetric | Same key for encryption and decryption | AES, DES, 3DES |
| Asymmetric | Public/private key pair | RSA, ECC |
| Hashing | One-way transformation (not reversible) | SHA-256, MD5 (not secure) |
| Hybrid | Combines symmetric & asymmetric | SSL/TLS (RSA + AES) |

**c. Tools:**

* **GPG**, **OpenSSL**, **VeraCrypt**, **AWS KMS**, **Azure Key Vault**, **HashiCorp Vault**.

**4. Describe Network Security in Cloud, Compute Security, and Storage Security**

**A. Network Security in Cloud:**

* **Virtual Private Cloud (VPC):** Isolated networks in cloud environments.
* **Subnets:** Public and private subnets to segregate resources.
* **Security Groups/Firewalls:** Control inbound/outbound traffic.
* **Network Access Control Lists (NACLs):** Stateless filtering at the subnet level.
* **DDoS Protection:** Services like AWS Shield, Azure DDoS Protection.

**B. Compute Security:**

* **Hardening OS:** Disable unused services, patching, minimal OS install.
* **Access Control:** IAM roles, MFA, SSH key-based access.
* **Monitoring:** Intrusion Detection Systems (IDS), log monitoring.
* **Isolation:** Use virtualization and container isolation (e.g., Docker, Kubernetes).

**C. Storage Security:**

* **Encryption at Rest:** AWS S3 default encryption, Azure Storage encryption.
* **Access Control:** IAM policies, storage ACLs, shared access signatures.
* **Backups:** Regular, secure backups with encryption.
* **Audit Trails:** Enable logging for access to storage resources.