**AWS Security Groups & NACLs (Network Access Control Lists)**

**1. Introduction**

* **Security Groups (SGs)**: Act as a **stateful firewall** (tracks connection state).
* **NACLs (Network Access Control Lists)**: Act as a **stateless firewall** (does not track connection state).

**2. Types of Firewalls**

**Stateful Firewall (Security Groups)**

* **Example**:
  + **Inbound (Ingress)**: User → SSH (Port 22) → Linux Server.
  + **Outbound (Egress)**: After authentication, response goes back via **same port (Port 22)**.
  + **Key Point**: Return traffic is **automatically allowed** without needing an explicit outbound rule.

**Stateless Firewall (NACLs)**

* **Example**:
  + **Inbound**: User → SSH (Port 22) → Linux Server.
  + **Outbound**: Response **does not use the same port**; requires **separate rule** (e.g., Ephemeral Ports 1024-65535).
  + **Key Point**: Must **explicitly allow inbound & outbound** traffic.

**3. Key Protocols & Ports**

| **Protocol** | **Port** | **Use Case** |
| --- | --- | --- |
| **SSH** | 22 | Secure Shell (Linux) |
| **RDP** | 3389 | Remote Desktop (Windows) |
| **HTTP** | 80 | Web Traffic |
| **HTTPS** | 443 | Secure Web Traffic |
| **ICMP** | - | Ping (Diagnostics) |

**4. Practical Demo: Security Groups**

**Steps:**

1. **Create Security Group**:
   * Allow **inbound SSH (Port 22)** only from your IP.
   * Initially, **no outbound rules** → No internet access.
2. **Test SSH**: Works (since inbound is allowed).
3. **Test Internet Access**: Fails (no outbound HTTP/HTTPS).
4. **Add Outbound Rules**:
   * Allow **HTTP (Port 80)** & **HTTPS (Port 443)** → Internet works.
   * Allow **ICMP** → Ping works.

**Key Observations:**

* **Stateful**: Return traffic allowed automatically.
* **Instance-Level**: Applied to **individual EC2 instances**.

**5. Practical Demo: NACLs**

**Steps:**

1. **Create NACL** and associate with **subnet**.
2. **Add Inbound Rule**: Allow **SSH (Port 22)**.
3. **Add Outbound Rule**: Must allow **Ephemeral Ports (1024-65535)** for response.
   * **Mistake**: Using same port (22) → Fails.
   * **Fix**: Allow high-range ports → Works.

**Key Observations:**

* **Stateless**: Must **explicitly allow return traffic**.
* **Subnet-Level**: Affects **all instances in subnet**.

**6. Security Groups vs NACLs**

| **Feature** | **Security Groups** | **NACLs** |
| --- | --- | --- |
| **Stateful?** | ✅ Yes | ❌ No |
| **Scope** | Instance-Level | Subnet-Level |
| **Rule Types** | Allow Only | Allow/Deny |
| **Return Traffic** | Auto-Allowed | Must be Explicitly Allowed |

**7. Real-World Example: 3-Tier Architecture**

* **Web Server (Public)**:
  + **Inbound**: HTTP/HTTPS (0.0.0.0/0) + SSH (Admin IP).
  + **Outbound**: All traffic (to App Server).
* **App Server (Private)**:
  + **Inbound**: Only from Web Server IP.
  + **Outbound**: Only to DB Server.
* **DB Server (Private)**:
  + **Inbound**: Only from App Server IP.

**Why?**

* **Security Groups** enforce **least privilege access**.
* **NACLs** add **subnet-level filtering**.

**8. Key Takeaways**

1. **Security Groups** = **Stateful** (return traffic auto-allowed).
2. **NACLs** = **Stateless** (must manually allow return traffic).
3. **Ephemeral Ports (1024-65535)** needed for NACL outbound rules.
4. **Practice!** Apply rules in AWS console for hands-on learning.

**Interview Questions (Basic to Advanced)**

**Basic Level (Fundamentals)**

**1. What is the difference between Security Groups and NACLs?**

**Answer**:

* **Security Groups (SGs)** are **stateful firewalls** (track connections) applied at the **instance level**. They only support **allow rules**.
* **NACLs (Network ACLs)** are **stateless firewalls** (do not track connections) applied at the **subnet level**. They support **allow/deny rules**.

**2. What is a stateful firewall?**

**Answer**:  
A stateful firewall **tracks connection states**. If an inbound rule allows traffic (e.g., SSH on Port 22), the **return traffic is automatically allowed** without needing an explicit outbound rule.

**3. What is a stateless firewall?**

**Answer**:  
A stateless firewall **does not track connections**. You must **explicitly allow inbound and outbound traffic** (e.g., NACLs require separate rules for request & response).

**4. Which ports are commonly used for SSH, RDP, and HTTP?**

**Answer**:

* **SSH** → Port 22
* **RDP** → Port 3389
* **HTTP** → Port 80
* **HTTPS** → Port 443

**Intermediate Level (Practical Scenarios)**

**5. Why does a ping (ICMP) fail even if HTTP/HTTPS works in a Security Group?**

**Answer**:

* **HTTP/HTTPS** use **TCP** (Port 80/443), while **ping** uses **ICMP protocol**.
* If the Security Group **does not allow ICMP**, ping will fail even if TCP traffic works.

**6. Why does SSH work in a Security Group but fail in an NACL?**

**Answer**:

* **Security Groups** are **stateful**, so return traffic is auto-allowed.
* **NACLs** are **stateless**, so you must **explicitly allow outbound ephemeral ports (1024-65535)** for the SSH response.

**7. How do you restrict access to an EC2 instance only from your IP?**

**Answer**:  
In the **Security Group inbound rule**, specify:

* **Type**: SSH (Port 22)
* **Source**: Your.IP.Address/32

**8. What happens if you block all outbound traffic in a Security Group?**

**Answer**:

* The instance **cannot send responses** (e.g., SSH replies, HTTP downloads).
* **Solution**: Allow necessary outbound rules (e.g., HTTP/HTTPS for web traffic).

**Advanced Level (Architecture & Troubleshooting)**

**9. How do NACLs process rules?**

**Answer**:  
NACLs evaluate rules **in order (lowest to highest rule number)** and **stop at the first match**. Example:

* **Rule 100**: Allow SSH (Port 22)
* **Rule 200**: Deny All  
  → SSH is allowed, but everything else is blocked.

**10. Why would you use both Security Groups and NACLs?**

**Answer**:

* **Security Groups** for **instance-level granular control** (e.g., allow SSH only for admins).
* **NACLs** for **subnet-wide filtering** (e.g., block malicious IPs at subnet level).

**11. How do you troubleshoot if an EC2 instance cannot connect to the internet?**

**Answer**:

1. **Check Security Groups**: Ensure **outbound HTTP/HTTPS (Port 80/443)** is allowed.
2. **Check NACLs**: Verify **both inbound & outbound rules** allow traffic.
3. **Check Route Tables**: Ensure the subnet has an **Internet Gateway (IGW)** route.

**12. What are ephemeral ports, and why are they important in NACLs?**

**Answer**:

* **Ephemeral Ports (1024-65535)** are temporary ports used for return traffic.
* **NACLs must allow these** because stateless firewalls **do not auto-allow responses**.

**13. How would you design security for a 3-tier architecture?**

**Answer**:

* **Web Tier (Public Subnet)**:
  + **SG**: Allow HTTP/HTTPS from anywhere, SSH only from admin IP.
  + **NACL**: Block malicious IPs.
* **App Tier (Private Subnet)**:
  + **SG**: Allow traffic only from Web Tier.
* **DB Tier (Private Subnet)**:
  + **SG**: Allow traffic only from App Tier.

**14. Can NACLs block traffic allowed by Security Groups?**

**Answer**:  
**Yes!** NACLs are evaluated **before Security Groups**. If NACL denies traffic, Security Group rules **won’t override it**.

**15. What is the default behavior of Security Groups and NACLs?**

**Answer**:

* **Security Groups**: **Deny all by default** (only explicitly allowed traffic passes).
* **NACLs**: **Allow all by default** (unless modified).

**Final Tip for Interviews**

* **For AWS roles**, expect **scenario-based questions** (e.g., "Why can’t my EC2 instance connect to S3?").
* **Always mention**:
  + **Stateful vs Stateless**
  + **Rule Evaluation Order (NACLs)**
  + **Ephemeral Ports**