# Securing and Troubleshooting Your Network

# At the core of the lesson

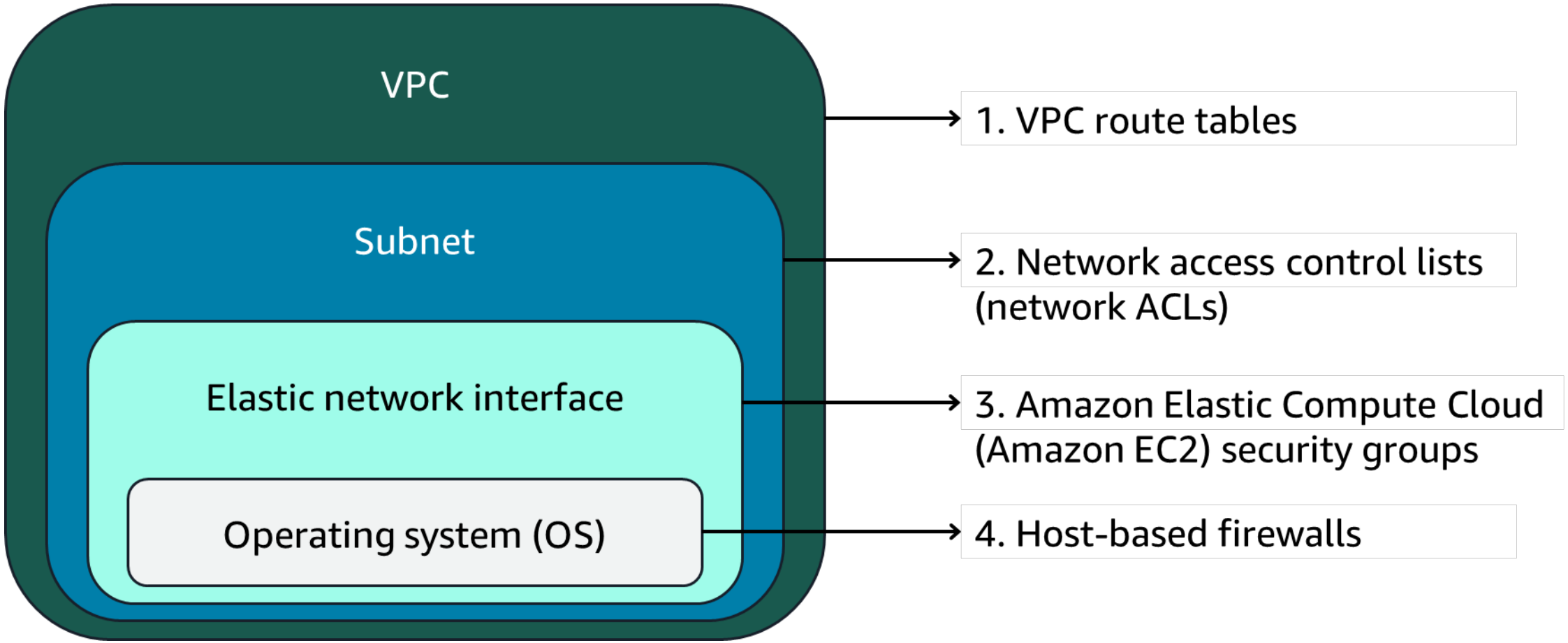
You will learn how to do the following:

- Describe the methods for securing a virtual private cloud (VPC).
- List the steps to troubleshoot common VPC connection issues.

# Securing your network

# Layered network defense

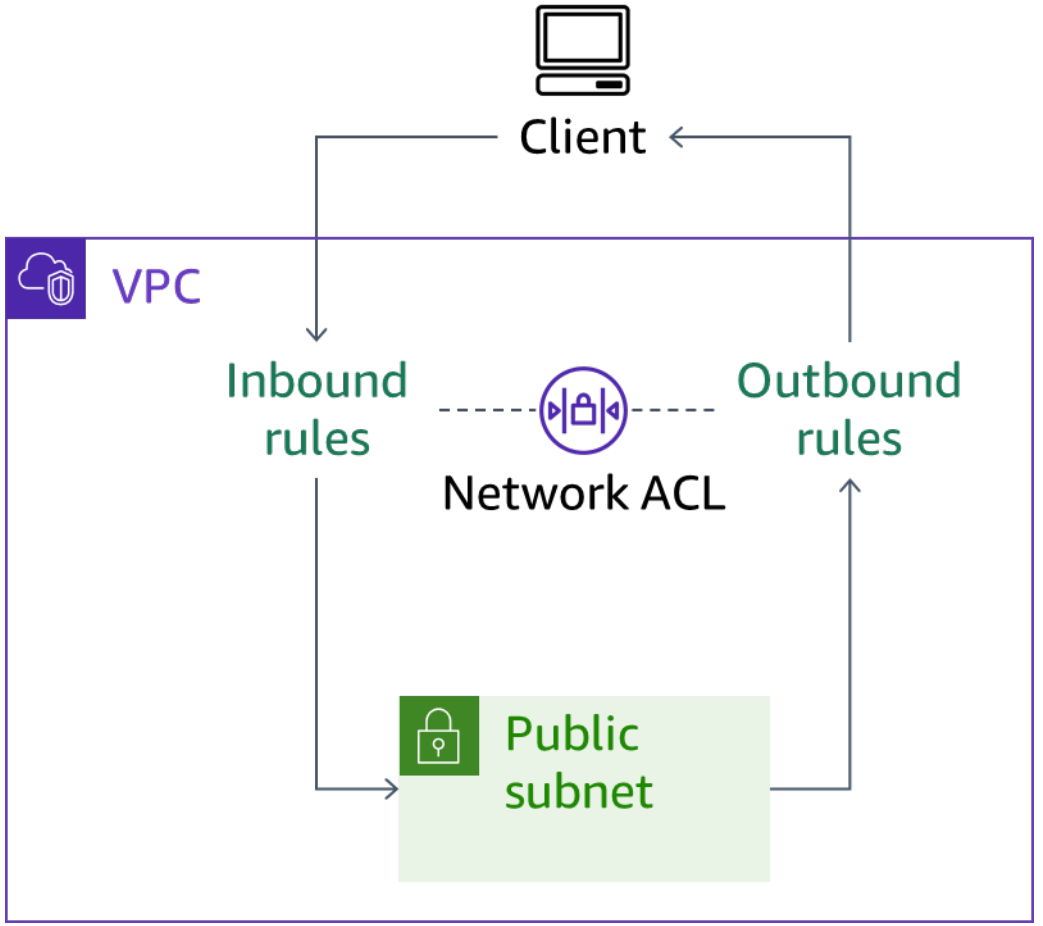
Secure your VPC at multiple levels.



# Network ACLs

A network ACL allows or denies traffic in and out of subnets and has the following characteristics:

- It defines traffic rules in an inbound rules table and an outbound rules table.
- It is stateless. Even if rules allow traffic to flow in one direction, you must explicitly allow responses to flow in the opposite direction.



# Default network ACL rule tables

The default network ACL allows all inbound and outbound traffic.

**Inbound rule table**

| Rule Number | Type | Protocol | Port Range | Source | Allow or Deny |
|---|---|---|---|---|---|
| 100 | ALL traffic | ALL | ALL | 0.0.0.0/0 | ALLOW |
| * | ALL traffic | ALL | ALL | 0.0.0.0/0 | DENY |

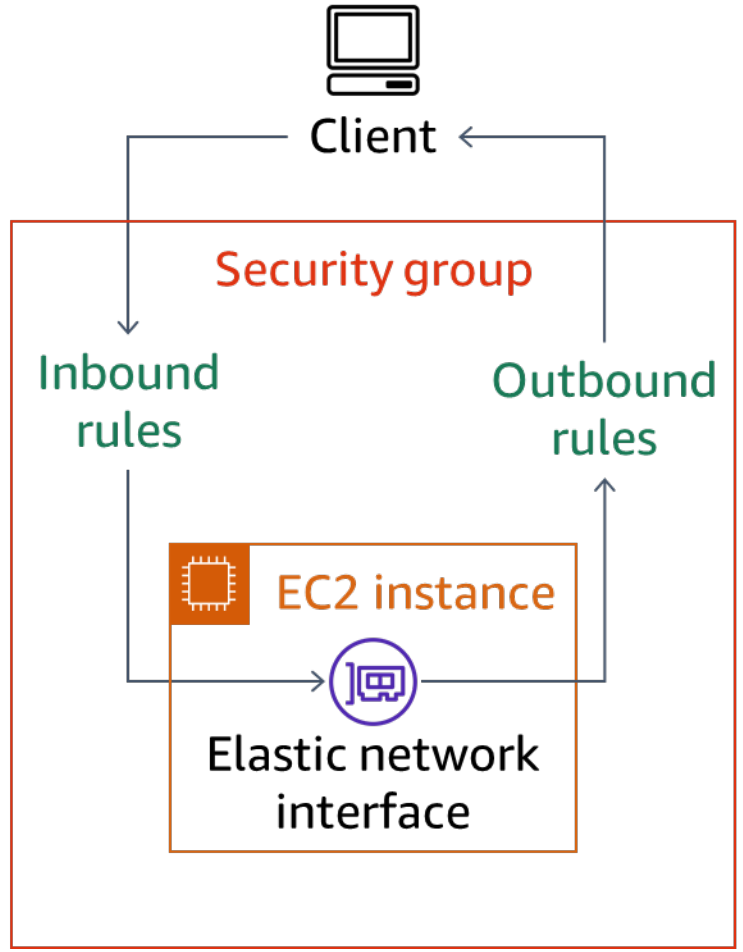
**Outbound rule table**

| Rule Number | Type | Protocol | Port Range | Destination | Allow or Deny |
|---|---|---|---|---|---|
| 100 | ALL traffic | ALL | ALL | 0.0.0.0/0 | ALLOW |
| * | ALL traffic | ALL | ALL | 0.0.0.0/0 | DENY |

# Security groups

A security group allows traffic to or from an elastic network interface and has the following characteristics:

- It defines traffic rules in an inbound rules table and an outbound rules table.
- It is configured by default to do the following:
  - Deny all inbound traffic.
  - Allow all outbound traffic.
  - Allow traffic between resources that are assigned to the same security group.
- It is stateful. If rules allow traffic to flow in one direction, responses can automatically flow in the opposite direction.



# Default security group rule tables

### Inbound rule table

| Type | Protocol | Port Range | Source |
|---|---|---|---|
| ALL traffic | ALL | ALL | sg-12345abcde<br>(ID of this security group) |

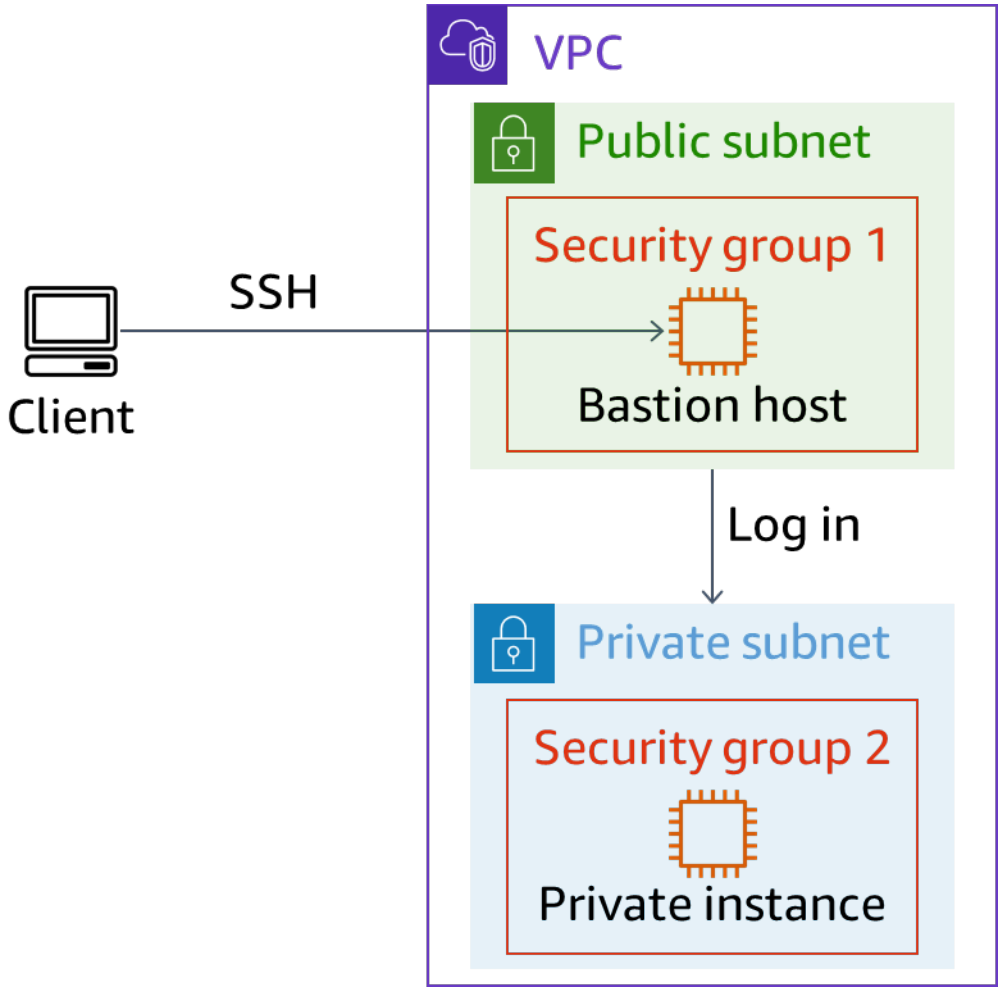
### Outbound rule table

| Type | Protocol | Port Range | Destination |
|---|---|---|---|
| ALL traffic | ALL | ALL | 0.0.0.0/0 |

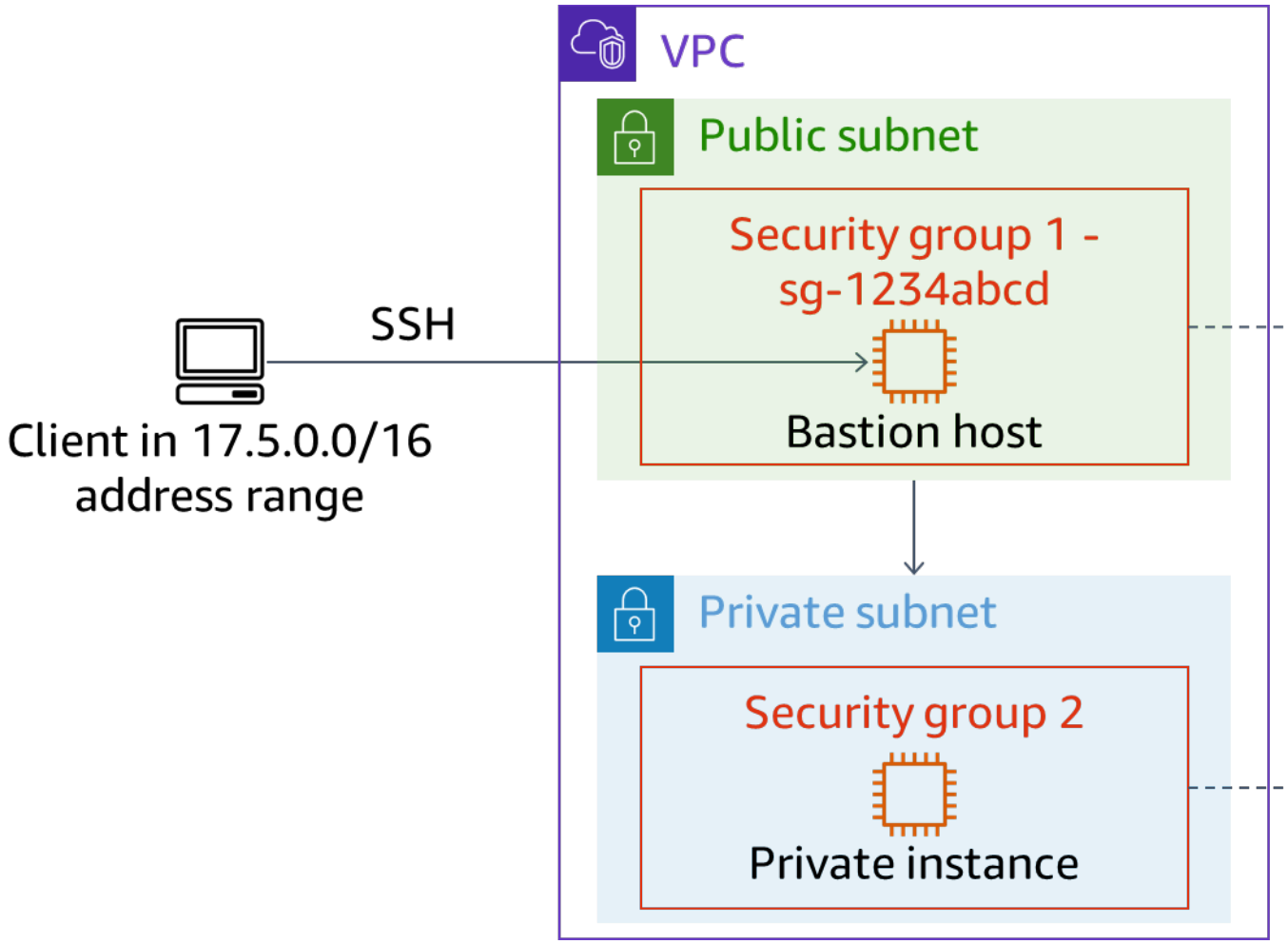
# Bastion host

A bastion host provides secure access from a public subnet to a private subnet and has the following characteristics:

- It is an EC2 instance.
- It provides a jump point to gain access to instances or resources in a private subnet from the internet.
- It requires a key pair for itself and the private instances that it connects to.



# Linux bastion host security group configuration example




**Security group 1 inbound rule table**

| Protocol | Port Range | Source |
|---|---|---|
| SSH | 22 | 17.5.0.0/16 |

**Security group 2 inbound rule table**

| Protocol | Port Range | Source |
|---|---|---|
| SSH | 22 | sg-1234abcd |

# Troubleshooting network connections on AWS

# Common troubleshooting tasks

- Verify that the instance is up and running. Check that it has passed both the System Status and Instance Status checks.
- Verify that the security groups that are associated with the instance allow connections for the required protocols and ports.
- Verify that the network ACLs that are associated with the subnet allow traffic from the necessary ports and protocols.
- Verify that the route table that is associated with the subnet has destination rules that point to the appropriate targets.

# Troubleshooting instance connections

Check the following if you cannot connect to an instance through the internet:

- Verify that the public IP address or Domain Name System (DNS) name that you are using is correct.
- Verify that the instance has a public IP address or Elastic IP address.
- Verify that an internet gateway is attached to the instance's VPC.
- Verify that the route table of the instance's subnet has a route rule for the destination 0.0.0.0/0 through the internet gateway.

# Troubleshooting SSH connections

Check the following if you cannot connect to an instance through Secure Shell (SSH):

- Verify that the instance's IP address or hostname is correct.
- Verify the instance connection credentials: instance private key, or username and password.
- Run the AWSSupport-TroubleshootSSH automation document to help you find and resolve the problem.

# Troubleshooting NAT

Check the following if your NAT configuration does not work:

- Verify that the route table has a route to the NAT instance or NAT gateway.
- If using a NAT instance, perform the following in addition:
  - Verify that the source or destination check is disabled.
  - Restart the NAT instance.

# Troubleshooting VPC peering

Check the following if you cannot reach resources in a peered network:

- Make sure that the peering request was approved.
- Verify that the security group rules allow network traffic between the peered VPCs.
- Check whether the network ACLs incorrectly deny all external traffic.

# Checkpoint questions

1. What are four methods to secure resources inside a VPC?
2. What kind of inbound and outbound traffic does the default security group allow or deny?
3. A network ACL is stateless. What does this mean?

# Key ideas

- Secure the network by using a layered design. A layered network can take advantage of the following:
  - Route tables to control traffic flow
  - Network ACLs to control traffic to and from subnets
  - Security groups to control traffic to hosts and services
- Secure administrative access using bastion hosts.
- When troubleshooting network connectivity issues, start with the following:
  - Verify that the resource is available.
  - Check for any blocking network ACLs or security groups.
  - Verify that routing is correct for the host or service.

# Thank you

Corrections, feedback, or other questions?
Contact us at https://support.aws.amazon.com/#/contacts/aws-training.
All trademarks are the property of their owners.