

## Introduction

In this lab step, you will create inbound and outbound rules for your private Network Access Control List (NACL). A NACL is a numbered list of rules that are evaluated in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL. As a best practice, you will start by creating rules with rule numbers that are multiples of 100. This can help with organization if you need to insert new rules later on, as there is room within the numbering scheme.

*Warning:* Although configuration is not difficult, it is easy to make mistakes or typos. For example, an incorrect digit for a CIDR block can break the lab. Take your time configuring the rules with the instructions below.

## Instructions

1. In the left navigation pane, click **Network ACLs** under **SECURITY**:



2. Select **Private-NACL** from the list of Network ACLs.

3. Click the **Inbound rules** tab below the table and click **Edit inbound rules**:



4. Click **Add new rule** and configure the following:

- **Rule number:** Enter *100*
- **Type:** Select **SSH**
- **Source:** Enter *10.0.20.0/24*
- **Allow / Deny:** Select **Allow** from the drop-down menu

5. For the second rule, click **Add new rule** and configure the following:

- **Rule number:** Enter *200*
- **Type:** Select **Custom TCP Rule**
- **Port Range:** Enter *1024-65535*
- **Source:** Enter *0.0.0.0/0*
- **Allow / Deny:** Select **Allow** from the drop-down menu

This will allow return traffic for the outbound rules you will add shortly (the range is specified as *1024-65535* because these are the available ports and not reserved). This enables resources inside the subnet to receive responses to their outbound traffic.

6. Click **Save changes**:

An orange rectangular button with the text "Save changes" in white.

7. Ensure the **Private-NACL** is still selected then click the **Inbound rules** tab below the table to verify your inbound rules match the following:

Inbound rules (3)							Edit inbound rules
<input type="text" value="Filter inbound rules"/>							< 1 > ⚙
Rule number	Type	Protocol	Port range	Source	Allow/Deny		
100	SSH (22)	TCP (6)	22	10.0.20.0/24	✓ Allow		
200	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	✓ Allow		
*	All traffic	All	All	0.0.0.0/0	✗ Deny		

Now that you've verified the inbound rules, you will move on to configure the outbound rules. Although the outbound IP addresses can be anything, the ports need to be 80 or 443. In short, operating system updates needed by instances in your private subnet could come from anywhere (0.0.0.0/0), but they will be downloaded over port 80 (HTTP) or 443 (HTTPS). You will need to add rules to account for each port.

8. With the **Private-NACL** still selected, switch to the **Outbound rules** tab and click **Edit outbound rules**.

9. Click **Add new rule** and configure the following:

- **Rule number:** Enter *100*
- **Type:** Select **HTTP** from the drop-down menu
- **Destination:** Enter *0.0.0.0/0*
- **Allow / Deny:** Select **Allow** from the drop-down menu

10. For the second outbound rule, click **Add new rule** and configure the following:

- **Rule number:** Enter *200*

- **Type:** Select **HTTPS** from the drop-down menu
- **Destination:** Enter *0.0.0.0/0*
- **Allow / Deny:** Select **Allow** from the drop-down menu

11. For the third outbound rule, click **Add new rule** and configure the following:

- **Rule number:** Enter *300*
- **Type:** Select **Custom TCP** from the drop-down menu
- **Port Range:** Enter *32768-61000*
- **Destination:** Enter *10.0.20.0/24* (The CIDR block of your public subnet)
- **Allow / Deny:** Select **Allow** from the drop-down menu

12. Click **Save changes**:

An orange rectangular button with the text "Save changes" in white, bold, sans-serif font.

13. Ensure the **Private-NACL** is still selected then click the **Outbound rules** tab below the table to verify your inbound rules match the following:

## Outbound rules (4)

Rule number ▾	Type ▾	Protocol ▾	Port range ▾	Destination ▾	Allow/Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	✓ Allow
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	✓ Allow
300	Custom TCP	TCP (6)	32768 - 61000	10.0.20.0/24	✓ Allow
*	All traffic	All	All	0.0.0.0/0	✗ Deny

When you add or remove rules from a network ACL, the changes are automatically applied to the subnets it is associated with. NACLs may take longer to propagate, as opposed to security groups, which take effect almost immediately.

*Note:* If troubleshooting efforts are required, sometimes adding an Inbound and Outbound Rule allowing ICMP from anywhere can help while issues are resolved. (The ping utility requires ICMP.)

## Summary

In this lab step, you configured the inbound and outbound rules for the private Network Access Control List.