

Network Access Control List (NACLs)



An (optional) layer of security that acts
As a **firewall** for controlling traffic **in and out of subnet(s)**



NACLs - Introduction

NACLs acts as a **virtual firewall** at the subnet level

VPCs automatically get a default NACL

Subnets are associated with NACLs. Subnets can only belong to a single NACL.

The screenshot shows the AWS NACL configuration interface. At the top, there are tabs for 'Details', 'Inbound Rules' (which is selected and highlighted with a red box), 'Outbound Rules', 'Subnet associations', and 'Tags'. Below the tabs is a button 'Edit inbound rules'. A red arrow points from the text 'Each NACL contains a set of rules that can allow or deny traffic into (inbound) and out of (outbound) subnets' to the 'Inbound Rules' tab. Another red arrow points from the text 'Rule # determines the order of evaluation. From lowest to highest. The highest rule # can be 32766 and its recommended to work in 10 or 100 increments.' to the 'Rule #' column in the table below. A red box highlights the 'Inbound Rules' table. The table has columns for Rule #, Type, Protocol, Port Range, Source, and Allow / Deny. It contains two rows: one for Rule # 100 with Type 'ALL Traffic', Protocol 'ALL', Port Range 'ALL', Source '0.0.0.0/0', and Action 'ALLOW'; and another for Rule # * with Type 'ALL Traffic', Protocol 'ALL', Port Range 'ALL', Source '0.0.0.0/0', and Action 'DENY'. A red arrow points from the text 'You can allow or deny traffic. You could block a single IP address (You can't do this with Security Groups)' to the 'Allow / Deny' column.

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Each NACL contains a set of rules that can **allow** or **deny** traffic **into (inbound)** and **out of (outbound)** subnets

Rule # determines the **order of evaluation**. From lowest to highest. The highest rule # can be 32766 and its recommended to work in 10 or 100 increments.

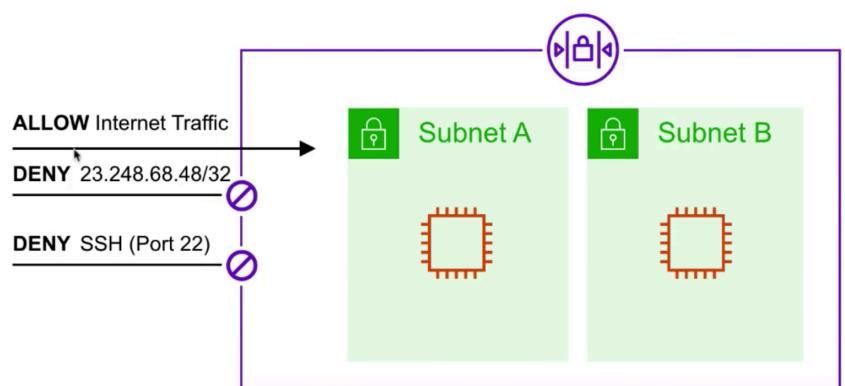
You can allow or deny traffic. You **could block a single IP address** (You can't do this with Security Groups)



NACLs - Use Case

We determine there is a malicious actor at a specific IP address is trying to access our instances so we block their IP

We never need to SSH into instances so we add a DENY for these subnets. This is just an additional measure in case our Security Groups SSH port was left open.





NACLs *CheatSheet*

- Network Access Control List is commonly known as NACL
- VPCs are automatically given a default NACL which allows **all** outbound and inbound traffic.
- Each subnet within a VPC must be associated with a NACL
- Subnets can only be associated with 1 NACL at a time. Associating a subnet with a new NACL will remove the previous association.
- If a NACL is not explicitly associated with a subnet, the subnet will automatically be associated with the default NACL.
- NACL has inbound and outbound rules (just like Security Groups).
- Rule can either **allow** or **deny** traffic. (unlike Security Groups which can only allow)
- NACLs are STATELESS (any allowed inbound traffic is also allowed outbound)
- When you create a NACLs it will deny all traffic by default
- NACLs contain a numbered list of rules that gets evaluated in order from lowest to highest.
- If you needed to block a single IP address you could via NACLs (Security Groups cannot deny)

