

Amazon VPC-4



CLARUSWAY
WAY TO REINVENT YOURSELF

Table of Content

- WORDPRESS WITH LAMP STACK ON VPC
- NACL

CLARUSWAY
WAY TO REINVENT YOURSELF

WORDPRESS WITH LAMP STACK ON VPC

Dynamic Website

Dynamic Website



Operating
System

Web Server

Database

Prg. Language

Setup Wordpress with Database

LAMP:



CLARUSWAY
WAY TO REINVENT YOURSELF

Operating
System

Web Server



Database

Progr. language

LAMP:



EC2 Amazon Linux 2



User Data



Another EC2
Instance

User Data

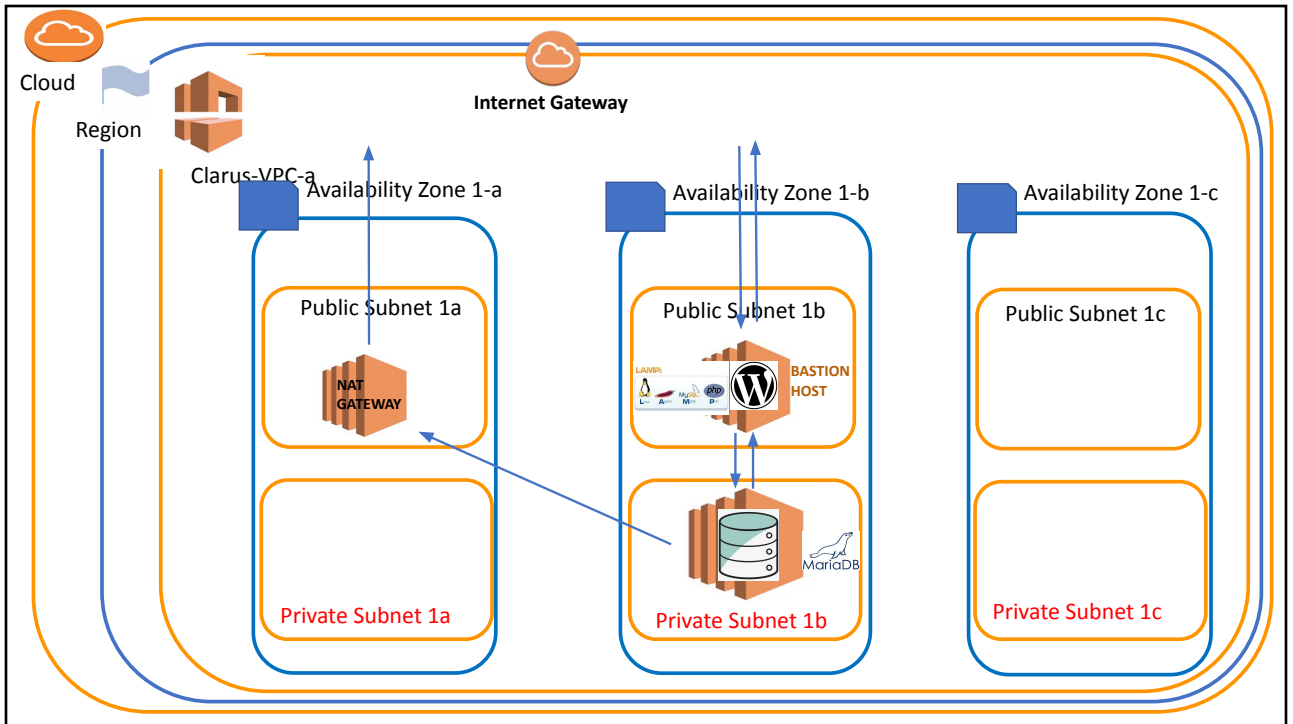


User Data

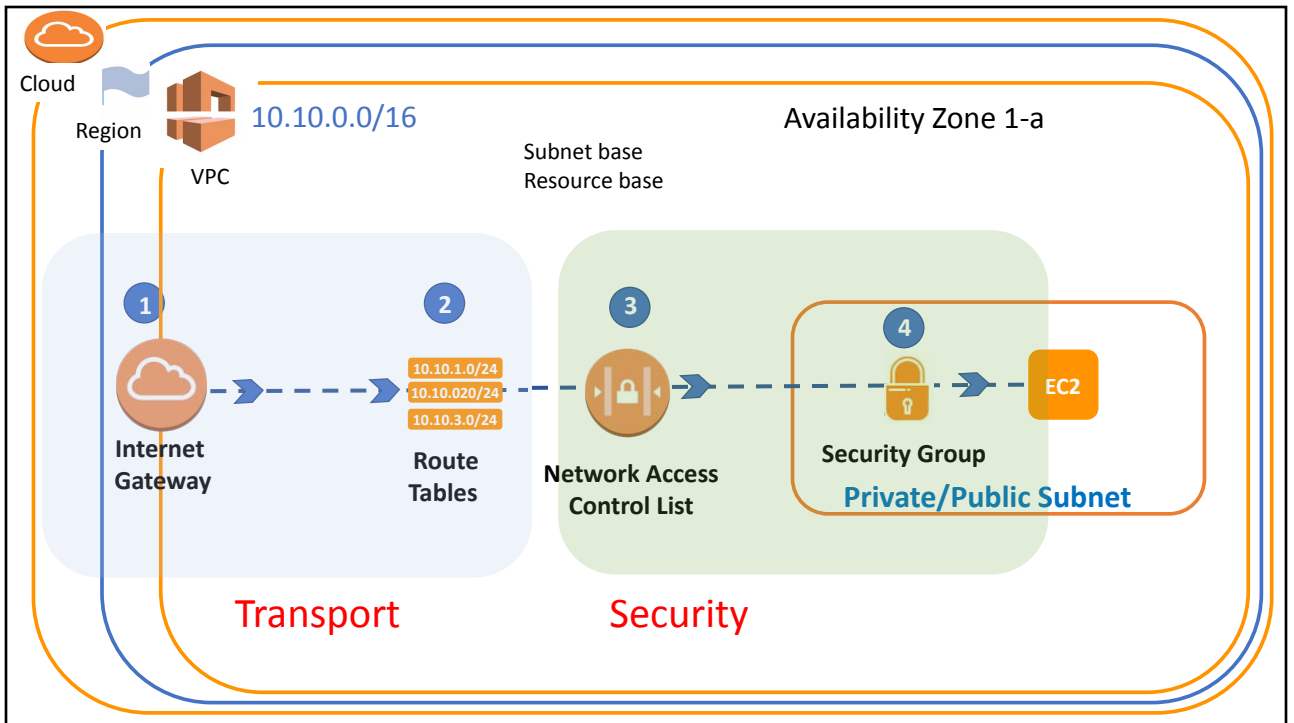
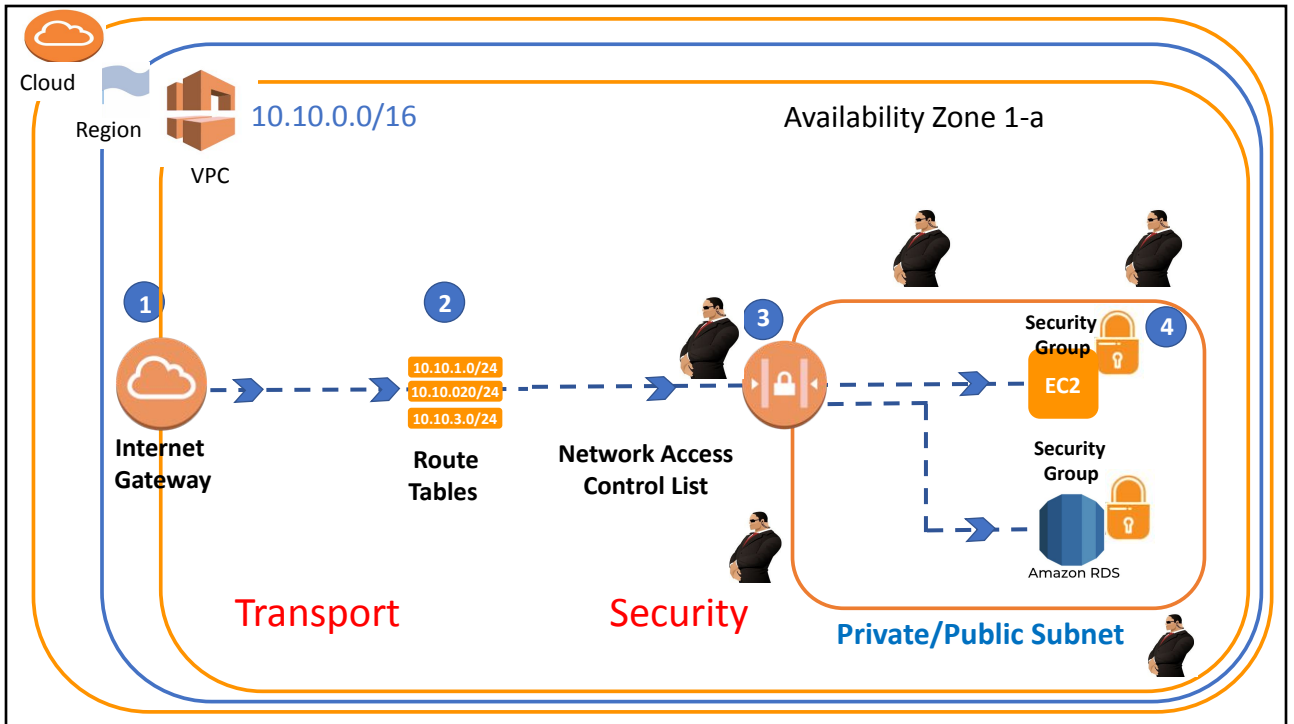


User Data





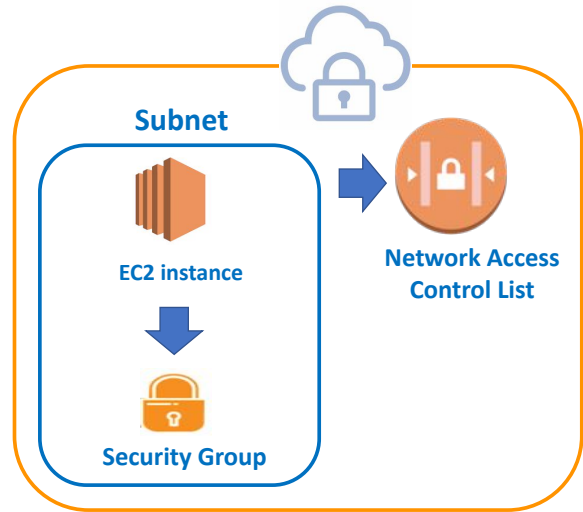
NACL (NETWORK ACCESS CONTROL LIST)



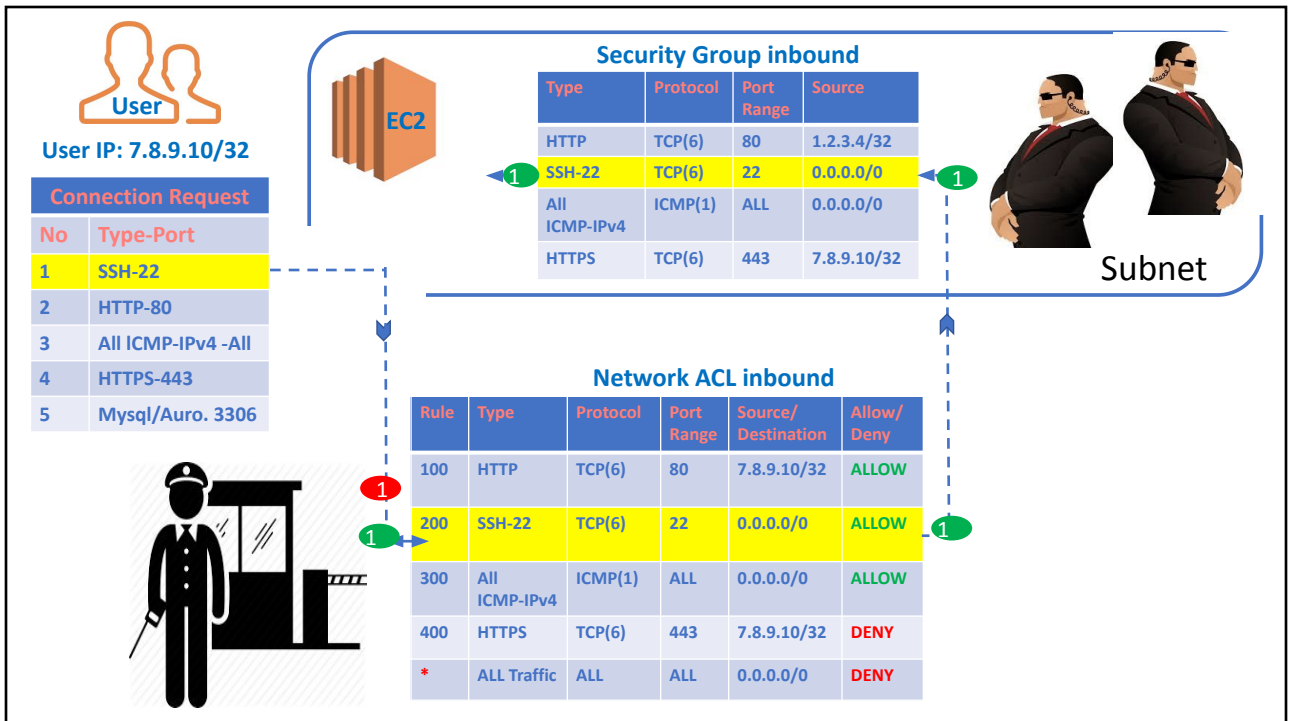
NACL (NETWORK ACCESS LISTS)

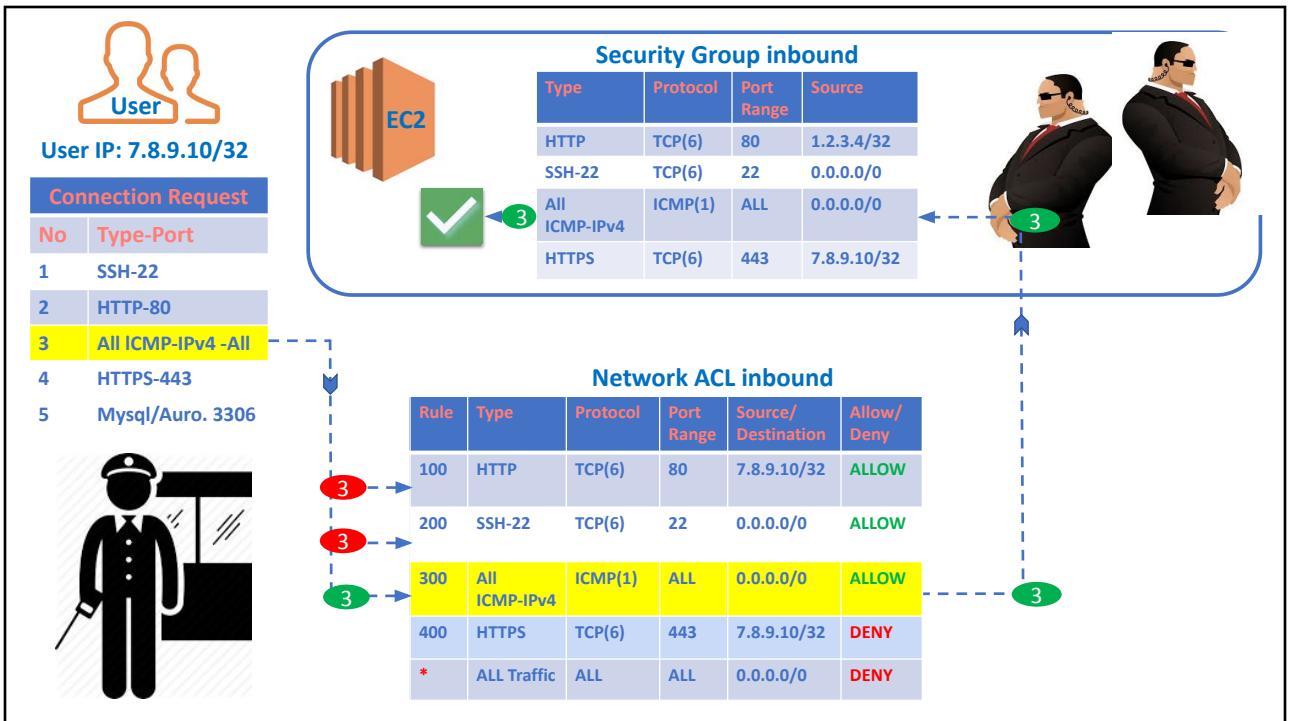
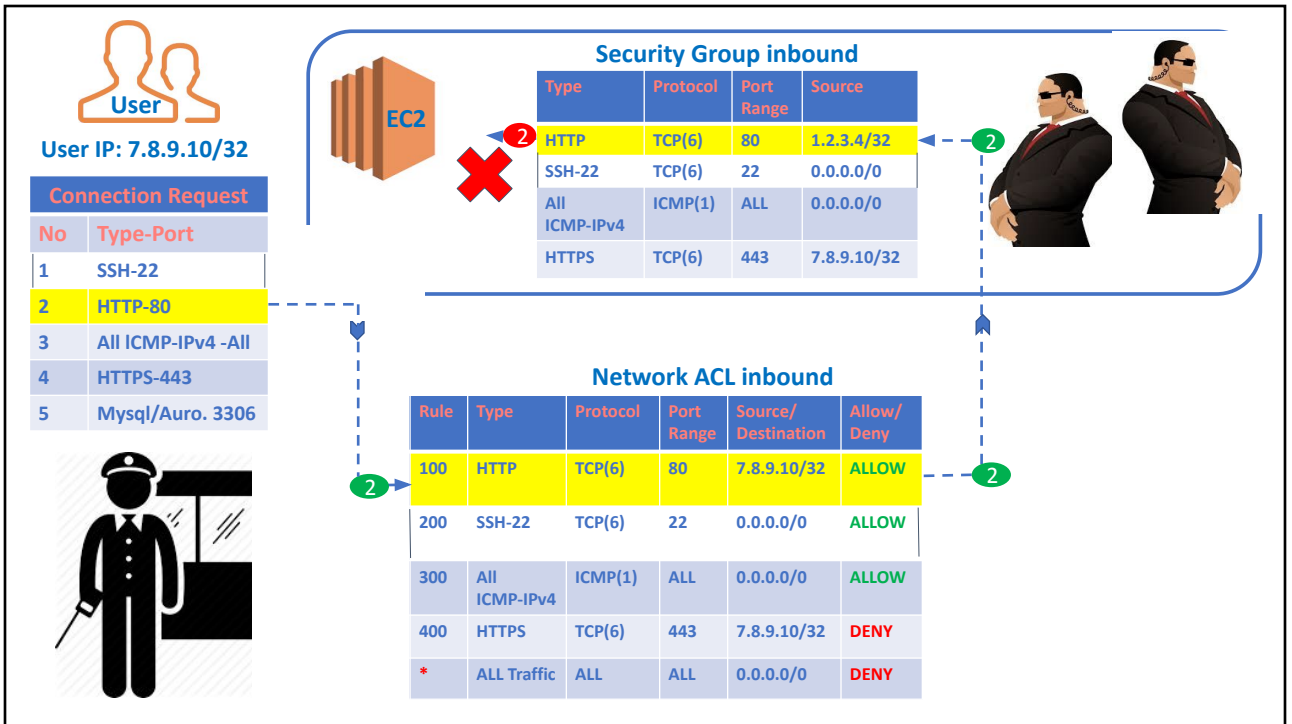
Subnet obeys the NACL rules

Resources obeys NACL and Sec. Group



CLARUSWAY
WAY TO REINVENT YOURSELF







User IP: 7.8.9.10/32

Connection Request

No	Type-Port
1	SSH-22
2	HTTP-80
3	All ICMP-IPv4 -All
4	HTTPS-443
5	Mysql/Auro. 3306



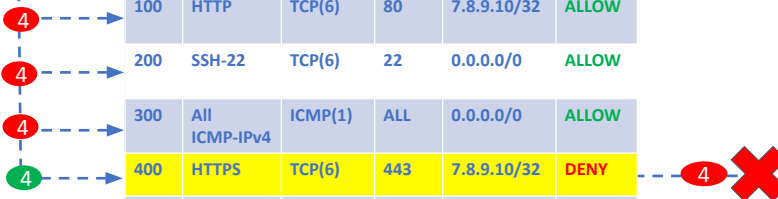
Security Group inbound

Type	Protocol	Port Range	Source
HTTP	TCP(6)	80	1.2.3.4/32
SSH-22	TCP(6)	22	0.0.0.0/0
All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0
HTTPS	TCP(6)	443	7.8.9.10/32



Network ACL inbound

Rule	Type	Protocol	Port Range	Source/Destination	Allow/Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY



User IP: 7.8.9.10/32

Connection Request

No	Type-Port
1	SSH-22
2	HTTP-80
3	All ICMP-IPv4 -All
4	HTTPS-443
5	Mysql/Auro. 3306



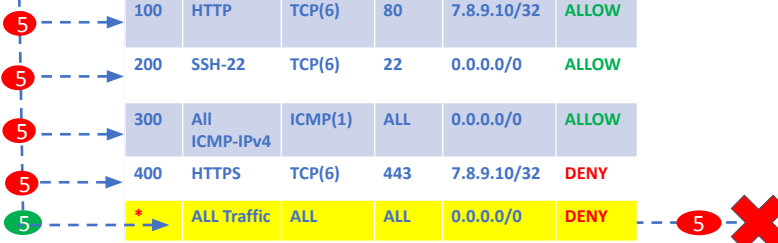
Security Group inbound

Type	Protocol	Port Range	Source
HTTP	TCP(6)	80	1.2.3.4/32
SSH-22	TCP(6)	22	0.0.0.0/0
All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0
HTTPS	TCP(6)	443	7.8.9.10/32



Network ACL inbound

Rule	Type	Protocol	Port Range	Source/Destination	Allow/Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY



(Stateful) **Security Group inbound**

Type	Protocol	Port Range	Source
HTTP	TCP(6)	80	1.2.3.4/32
SSH-22	TCP(6)	22	0.0.0.0/0
All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0
HTTPS	TCP(6)	443	7.8.9.10/32

ALLOW Only

Network ACL inbound (Stateless)

Rule	Type	Protocol	Port Range	Source	Allow/Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY



(Stateless) **Network ACL outbound**

Rule	Type	Protocol	Port Range	Destination	Allow/Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	Custom TCP	TCP(6)	32768 - 65535	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

EPHEMERAL PORT

NACLs are stateless. This means that you are required to have a rule for inbound AND outbound traffic. So, if you want to allow your EC2 instance to serve HTTP traffic, you will need to allow port 80 inbound and ports 1024 – 65535 outbound. But where 1024 – 65535 came from.

The ports 1024 – 65535 are called the “ephemeral ports”.

These ports are randomly selected to allow return traffic for a request. So, if a request comes to the server on port 80, the request also specifies a random port between 1024 – 65535 for the return traffic.

▶ NACL TABLES

Let's get our hands dirty!

- NACL Tables