

# LAB2 - Network Security

In this Lab you will configure Security Group for your Internet-facing server, and break DDoS attack to your server.

---

## Step 1 - Install Apache in your EC2

- Connect to your EC2 over SSH.
- Install all updates: `sudo yum update -y`
- Install Apache: `sudo yum install httpd -y`
- Start a httpd service: `sudo service httpd start`

---

## Step 2 - Check your Website from the Internet

- In AWS GUI go to your EC2 instance.
- In the Description tab look for Public DNS (IPv4)
- Copy the name to the clipboard.
- Open Web Browser on your computer and paste the address (connection should fail)

---

## Step 3 - Configure EC2 instance's Security Group

- In the Description tab of your EC2 look for Security Groups.
- Press "view inbound rules".
- Click on your security group name

Security groups  . [view inbound rules](#)

- Go to Inbound tab and press Edit -> Add Rule
- Add new rule:
  - Type: HTTP
  - Source: Anywhere
- Press Save

Edit inbound rules

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	My IP	e.g. SSH for Admin Desktop
HTTP	TCP	80	Anywhere	e.g. SSH for Admin Desktop

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

CancelSave

- Switch back to your web browser and connect to your URL.

---

## Step 4 - Block DDoS

Imagine situation, where your website is under DDoS attack. You need to act fast. You need to find IP of the attacker and block him.

- Jump into ssh console of your EC2
- Install tcpdump: `sudo yum install tcpdump -y`
- Check network interface id to listen on: `ifconfig`
- Listen for all incoming packages on port 80: `tcpdump -i eth0 'port 80'`
- Try to find attacker IP address
- Do not brake a tcpdump.

---

## Step 5 - Block traffic from IP address of attacker

- Go to Services -> EC2
- Select your EC2 instance
- In Description tab look for Subnet ID and copy the value
- Go to Services VPC -> Subnets
- In search filed paste subnet ID
- Select your subnet and go to Network ACL tab
- Click on Network ACL name (you will be forward to ACLs sections)
- Select your ACL and Inbound Rules tab
- Press Edit and Add another rule
  - Rule: Number must be lower then Allow All rule.
  - Type: All traffic
  - Protocol: All
  - Source: IP address that need to be blocked. (with /32 at the end)
  - Allow/Deny: DENY
- Press Save

Summary

Inbound Rules

Outbound Rules

Subnet Associations

Tags

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Cancel

Save

View: All rules

Rule #	Type	Protocol	Port Range	Source		Allow / Deny	Remove
100	ALL Traffic	ALL	ALL	0.0.0.0/0	i	ALLOW	✕
10	ALL Traffic	ALL	ALL	: 186/32	i	DENY	✕

Add another rule

- Go back ssh console and verify is traffic from attacker is blocked.
- (The connections flood should be stopped now).