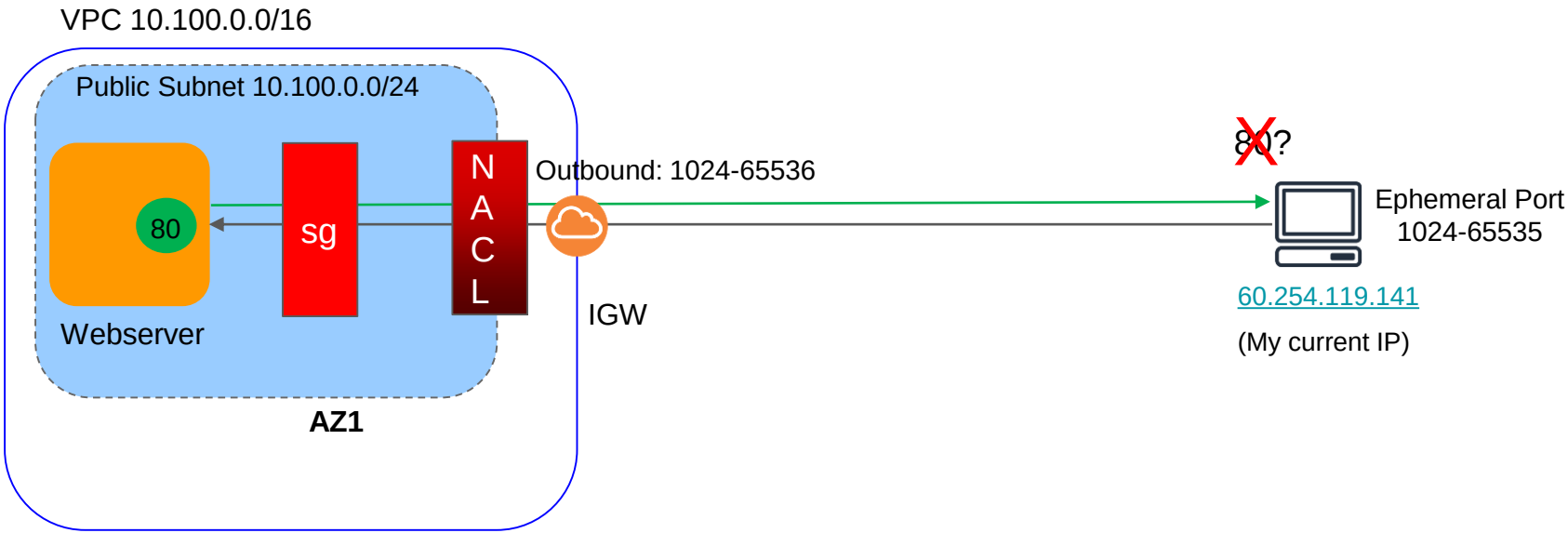
Network ACL



Copyright@kvriksh2019

Network ACL

Default Inbound Rules

Inbound rules (2)

Filter inbound rules

Rule number	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

Default Outbound Rules

Outbound rules (2)

Filter outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Copyright@kvriksh2019

Network ACL

1. Let's remove the default inbound allow rules from NACL
2. Let's remove the default outbound allow rules from NACL
3. Let's allow only MyIP in inbound rule for port 80
4. Let's allow only MyIP in outbound rule for port 80
5. Let's allow only MyIP in outbound rule for ephemeral port range 1024-65535
6. Let's block only MyIP and allow internet traffic

Note: The ephemeral port range depends on the type of the client

- Many Linux kernels (including the Amazon Linux kernel) use ports 32768-61000.
- Requests originating from Elastic Load Balancing use ports 1024-65535.
- Windows operating systems through Windows Server 2003 use ports 1025-5000.
- Windows Server 2008 and later versions use ports 49152-65535.
- A NAT gateway uses ports 1024-65535.
- AWS Lambda functions use ports 1024-65535.

Copyright@kvriksh2019