A CLOUD GURU

Network Access Control Lists vs Security Groups - LAB

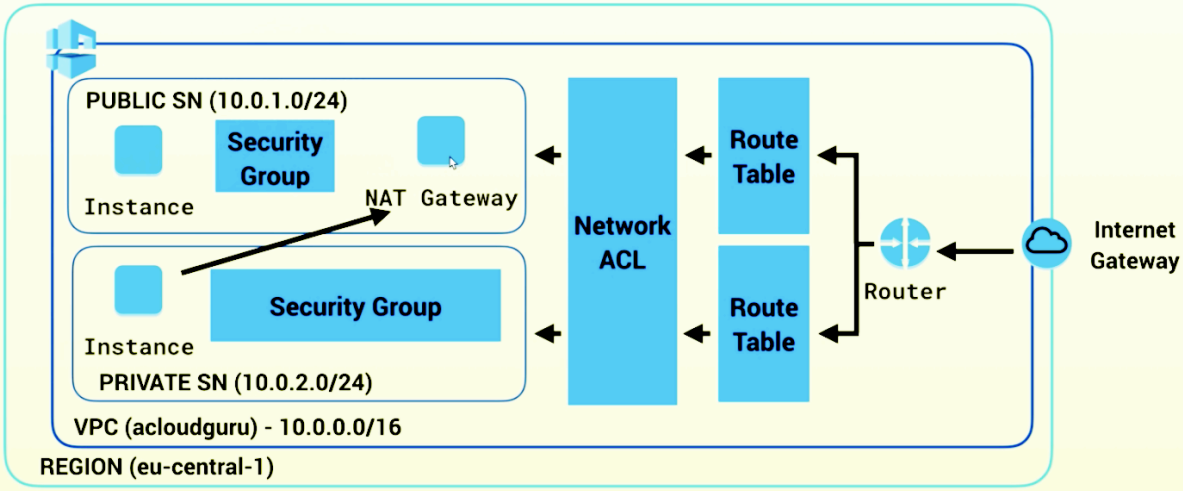
Ryan Kroonenburg
AWS COMMUNITY HERO & ALEXA CHAMPION
FOUNDER OF A CLOUD GURU

NAT INSTANCES & NAT GATEWAYS

NAT Gateways Explained

A CLOUD GURU

VPC with Public & Private Subnet(s)



VPC Dashboard

Filter by VPC:

Select a VPC

Virtual Private Cloud

- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

Security

- Network ACLs

Create network ACL | Actions

Filter by tags and attributes or search by keyword

1 to 2 of 2

Name	Network ACL ID	Associated with	Default	VPC	Owner
	acl-07b1a174772c...	2 Subnets	Yes	vpc-07999b20eeffad16b | acloudguruVPC	888791739481
	acl-a207f2c9	3 Subnets	Yes	vpc-cb3d33a3	888791739481

Network ACL: acl-07b1a174772c5aab3

Details | Inbound Rules | Outbound Rules | Subnet associations | Tags

Network ACL ID acl-07b1a174772c5aab3

Associated with 2 Subnets

Default Yes

VPC vpc-07999b20eeffad16b | acloudguruVPC

VPC Dashboard

Filter by VPC:

Select a VPC

Virtual Private Cloud

- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

Security

- Network ACLs
- Security Groups

Virtual Private Network (VPN)

- Customer Gateways
- Virtual Private Gateways
- Site-to-Site VPN Connections

Create network ACL | Actions

Filter by tags and attributes or search by keyword

1 to 2 of 2

Name	Network ACL ID	Associated with	Default	VPC	Owner
	acl-07b1a174772c...	2 Subnets	Yes	vpc-07999b20eeffad16b | acloudguruVPC	888791739481
	acl-a207f2c9	3 Subnets	Yes	vpc-cb3d33a3	888791739481

Details | Inbound Rules | Outbound Rules | Subnet associations | Tags

Edit inbound rules

View All rules

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

Pause

NAT Gateways
Peering Connections

Security
Network ACLs
Security Groups

Virtual Private Network (VPN)
Customer Gateways
Virtual Private Gateways
Site-to-Site VPN Connections

Network ACL: acl-07b1a174772c5aab3

Details | Inbound Rules | **Outbound Rules** | Subnet associations | Tags

Edit outbound rules

View All rules

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

Feedback English (US) Privacy Policy Terms of Use

Network ACLs > Create network ACL

Create network ACL

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Name tag MyWebNACL

VPC* |

Filter by attributes

vpc-cb3d33a3

vpc-07999b20eeffad16b acloudguruVPC

* Required

Cancel Create

VPC Dashboard

Filter by VPC:

Select a VPC

Virtual Private Cloud

- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

Security

- Network ACLs
- Security Groups

Virtual Private Network (VPN)

- Customer Gateways
- Virtual Private Gateways
- Site-to-Site VPN Connections

Create network ACL | Actions

Filter by tags and attributes or search by keyword

1 to 3 of 3

Name	Network ACL ID	Associated with	Default	VPC	Owner
MyWebNACL	acl-071ee8e42283...	subnet-0fcd3d990...	No	vpc-07999b20eeffad16b | acloudguruVPC	888791739481
	acl-07b1a174772c...	subnet-004c93c77...	Yes	vpc-07999b20eeffad16b | acloudguruVPC	888791739481
	acl-a207f2c9	3 Subnets	Yes	vpc-cb3d33a3	888791739481

Network ACL: acl-071ee8e42283678d9

Details | Inbound Rules | Outbound Rules | Subnet associations | Tags

Edit inbound rules

View: All rules

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

Network ACLs > Edit inbound rules

Edit inbound rules

Network ACL acl-071ee8e42283678d9

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	Custom TCP Rule	TCP (6)	80	0.0.0.0/0	ALLOW
200	Custom TCP Rule	TCP (6)	443	0.0.0.0/0	ALLOW
300	Custom TCP Rule	TCP (6)	22	0.0.0.0/0	ALLOW

Add Rule

* Required

Cancel | Save

Network ACLs > Edit outbound rules

Edit outbound rules

Network ACL acl-071ee8e42283678d9

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	Custom TCP Rule	TCP (6)	80	0.0.0.0/0	ALLOW
200	Custom TCP Rule	TCP (6)	443	0.0.0.0/0	ALLOW
300	Custom TCP Rule	TCP (6)	1024-65535	0.0.0.0/0	ALLOW

Add Rule

* Required

Cancel Save

Details | Inbound Rules | Outbound Rules | Subnet associations | Tags

Edit inbound rules

View All rules

Rule #	Type	Protocol	Port Range	Source	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	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

Ephemeral port

An ephemeral port is a short-lived transport protocol port for Internet Protocol communications. Ephemeral ports are allocated automatically from a predefined range by the IP stack software. Wikipedia

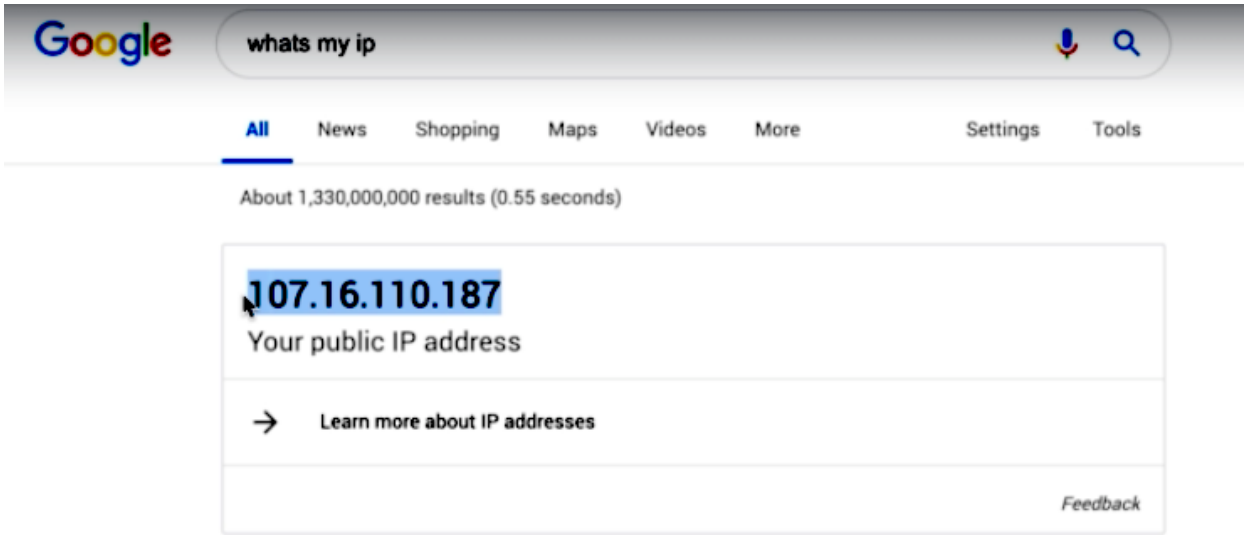
Ephemeral Ports

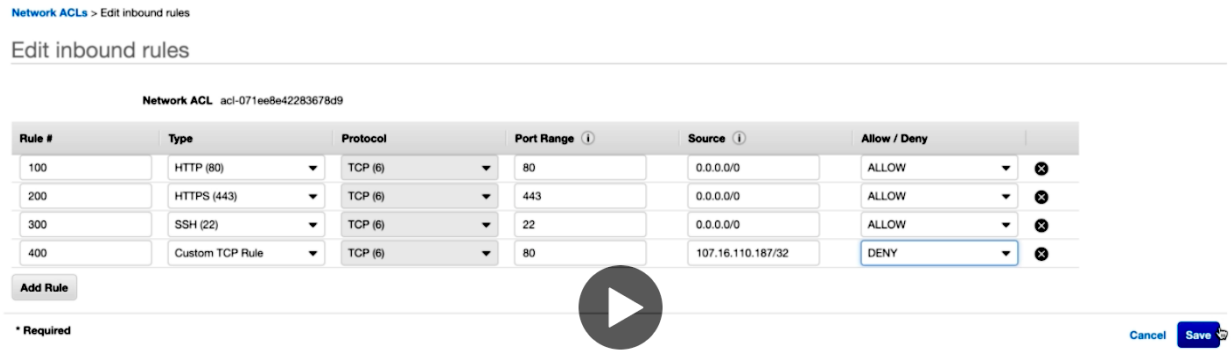
The example network ACL in the preceding section uses an ephemeral port range of 32768-65535. However, you might want to use a different range for your network ACLs depending on the type of client that you're using or with which you're communicating.

The client that initiates the request chooses the ephemeral port range. The range varies depending on the client's operating system. 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. For example, if a request comes into a web server in your VPC from a Windows XP client on the Internet, your network ACL must have an outbound rule to enable traffic destined for ports 1025-5000.

If an instance in your VPC is the client initiating a request, your network ACL must have an inbound rule to enable traffic destined for the ephemeral ports specific to the type of instance (Amazon Linux, Windows Server 2008, and so on).

In practice, to cover the different types of clients that might initiate traffic to public-facing instances in your VPC, you can open ephemeral ports 1024-65535. However, you can also add rules to the ACL to deny traffic on any malicious ports within that range. Ensure that you place the DENY rules earlier in the table than the ALLOW rules that open the wide range of ephemeral ports.


Google
whats my ip
All
News
Shopping
Maps
Videos
More
Settings
Tools
About 1,330,000,000 results (0.55 seconds)
107.16.110.187
Your public IP address
Learn more about IP addresses
Feedback


Network ACLs > Edit inbound rules
Edit inbound rules
Network ACL acl-071ee8e42283678d9
Rule # | Type | Protocol | Port Range | Source | 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 | SSH (22) | TCP (6) | 22 | 0.0.0.0/0 | ALLOW
400 | Custom TCP Rule | TCP (6) | 80 | 107.16.110.187/32 | DENY
Add Rule
* Required
Cancel
Save

Edit inbound rules

View All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
99	HTTP (80)	TCP (6)	80	107.16.110.187/32	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	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

This site can't be reached

18.216.240.182 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_TIMED_OUT

Details

Reload

Hello Cloud Gurus!

Network ACLs > Edit inbound rules

Edit inbound rules

Network ACL acl-0dd19e059b3a3e964

Rule #	Type	Protocol	Port Range	Source	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	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
400	Custom TCP Rule	TCP (6)	1024 - 65535	0.0.0.0/0	ALLOW

```
[root@ip-10-0-1-43 html]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                                               | 2.4 kB  00:00:00
Resolving Dependencies
--> Running transaction check
---> Package gnupg2.x86_64 0:2.0.22-5.amzn2.0.3 will be updated
---> Package gnupg2.x86_64 0:2.0.22-5.amzn2.0.4 will be an update
---> Package kernel.x86_64 0:4.14.173-137.228.amzn2 will be installed
---> Package langtable.noarch 0:0.0.31-3.amzn2 will be updated
---> Package langtable.noarch 0:0.0.31-4.amzn2 will be an update
---> Package langtable-data.noarch 0:0.0.31-3.amzn2 will be updated
---> Package langtable-data.noarch 0:0.0.31-4.amzn2 will be an update
---> Package langtable-python.noarch 0:0.0.31-3.amzn2 will be updated
---> Package langtable-python.noarch 0:0.0.31-4.amzn2 will be an update
---> Package libfastjson.x86_64 0:0.99.4-2.amzn2.0.2 will be updated
---> Package libfastjson.x86_64 0:0.99.4-3.amzn2 will be an update
---> Package libtirpc.x86_64 0:0.2.4-0.10.amzn2.0.2 will be updated
---> Package libtirpc.x86_64 0:0.2.4-0.16.amzn2 will be an update
--> Finished Dependency Resolution
```

NETWORK ACCESS CONTROL LISTS VS SECURITY GROUPS

Exam Tips

A CLOUD GURU

Remember the following for your exam;

- Your VPC automatically comes with a default network ACL, and by default it allows all outbound and inbound traffic.
- You can create custom network ACLs. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.
- Block IP Addresses using network ACLs not Security Groups

Exam Tips

Remember the following for your exam;

- You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.
- Network ACLs contain a numbered list of rules that is evaluated in order, starting with the lowest numbered rule.
- Network ACLs have separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa.)