

Difference between NACL vs SG

TASK PERFORM SG (STATEFULL)

CREATE 1 EC2 INSTANCE

Instances (1) [Info](#) Refresh Connect Instance state Actions Launch instances

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
<input type="checkbox"/>	webserver	i-0858921053edffea1	Running	t2.micro	2/2 checks passed		ap-south-1a	ec2-13-233-24

If remove the default outbound rule from sg and see whether you are able to RDP or not.

Outbound security group rules successfully modified on security group (sg-0e1c79f96231c42dc | web-sg)

[Details](#)

Security Groups (1/2) [Info](#) Refresh Actions Export security groups to CSV Create security group

<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description	Owner
<input type="checkbox"/>	-	sg-0dbe4c9d1877e20de	default	vpc-00747eff45a5d528d	default VPC security gr...	65920232663

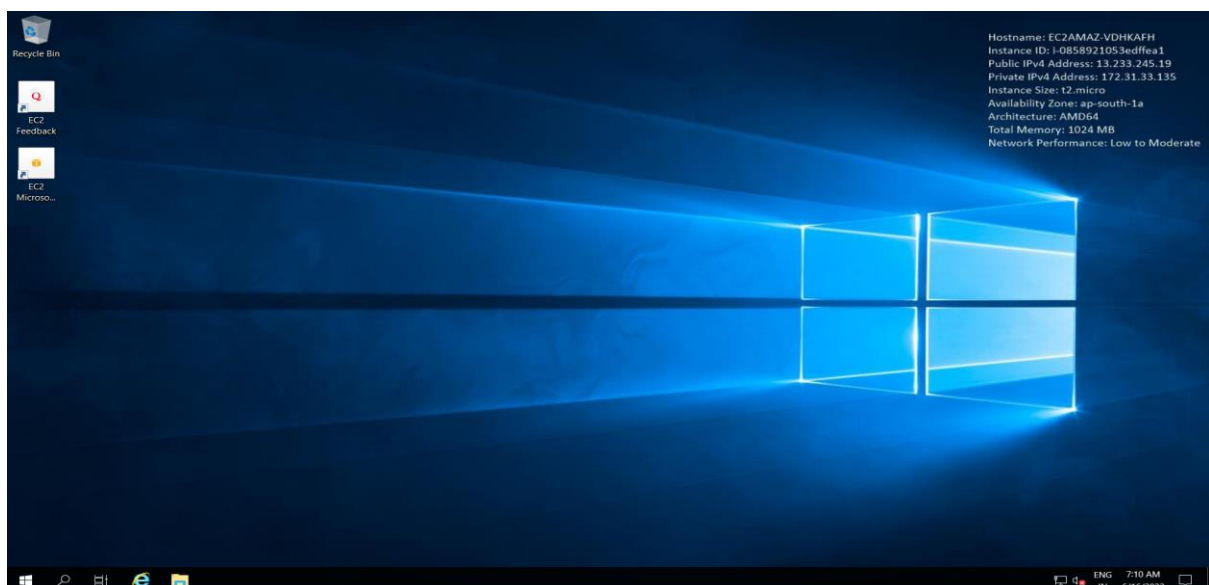
sg-0e1c79f96231c42dc - web-sg

[Details](#) [Inbound rules](#) [Outbound rules](#) [Tags](#)

Outbound rules Refresh Manage tags Edit outbound rules

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range
No security group rules found						

Check SUCCESSFULLY CONNECTED



Difference between NACL vs SG

If add new inbound rule for all ICMP ipv4 traffic in to sg

The screenshot shows the AWS Management Console for Security Groups. The 'Inbound rules' tab is selected, showing a table of inbound rules. The first rule is highlighted, showing it allows all ICMP traffic from any IP address.

Name	Security group ID	Security group name	VPC ID	Description	Owner
-	sg-0e1c79f96231c42dc	web-sg	vpc-00747eff45a5d528d	launch-wizard-1 create...	659202326636

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-00564c8b498d02cf3	IPv4	All ICMP - IPv4	ICMP	All

Try to ping windows instance which you created form your local system

```
C:\Users\Vivek Gandhi>ping 13.233.245.19

Pinging 13.233.245.19 with 32 bytes of data:
Reply from 13.233.245.19: bytes=32 time=119ms TTL=112
Reply from 13.233.245.19: bytes=32 time=136ms TTL=112
Reply from 13.233.245.19: bytes=32 time=140ms TTL=112
Reply from 13.233.245.19: bytes=32 time=149ms TTL=112
```

NOT GOING PING WINDOWS INSTANCE TO GOOGLE

```
C:\Users\Administrator>ping www.google.com

Pinging www.google.com [142.250.192.68] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Difference between NACL vs SG

TASK PERFORM NACL (STATELESS)

Go to nacl and see what are the default entry inbound and outbound rules

Network ACLs (1/1) Info Refresh Actions Create network ACL

Filter network ACLs

<input checked="" type="checkbox"/>	Name	Network ACL ID	Associated with	Default	VPC ID
<input checked="" type="checkbox"/>	-	acl-0603e115c692b69...	3 Subnets	Yes	vpc-00747eff45a5d528d

acl-0603e115c692b6961

Details **Inbound rules** Outbound rules Subnet associations Tags

Inbound rules (2) Edit inbound rules

Filter inbound rules

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

Network ACLs (1/1) Info Refresh Actions Create network ACL

Filter network ACLs

<input checked="" type="checkbox"/>	Name	Network ACL ID	Associated with	Default	VPC ID
<input checked="" type="checkbox"/>	-	acl-0603e115c692b69...	3 Subnets	Yes	vpc-00747eff45a5d528d

acl-0603e115c692b6961

Details Inbound rules **Outbound rules** Subnet associations Tags

Outbound rules (2) Edit outbound rules

Filter outbound rules

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

Go to inbound rule and create to rules 1 - allow rdp 2 - deny all traffic

Network ACLs (1/1) Info Refresh Actions Create network ACL

Filter network ACLs

<input checked="" type="checkbox"/>	Name	Network ACL ID	Associated with	Default	VPC ID
<input checked="" type="checkbox"/>	-	acl-0603e115c692b69...	3 Subnets	Yes	vpc-00747eff45a5d528d

acl-0603e115c692b6961

Details **Inbound rules** Outbound rules Subnet associations Tags

Inbound rules (3) Edit inbound rules

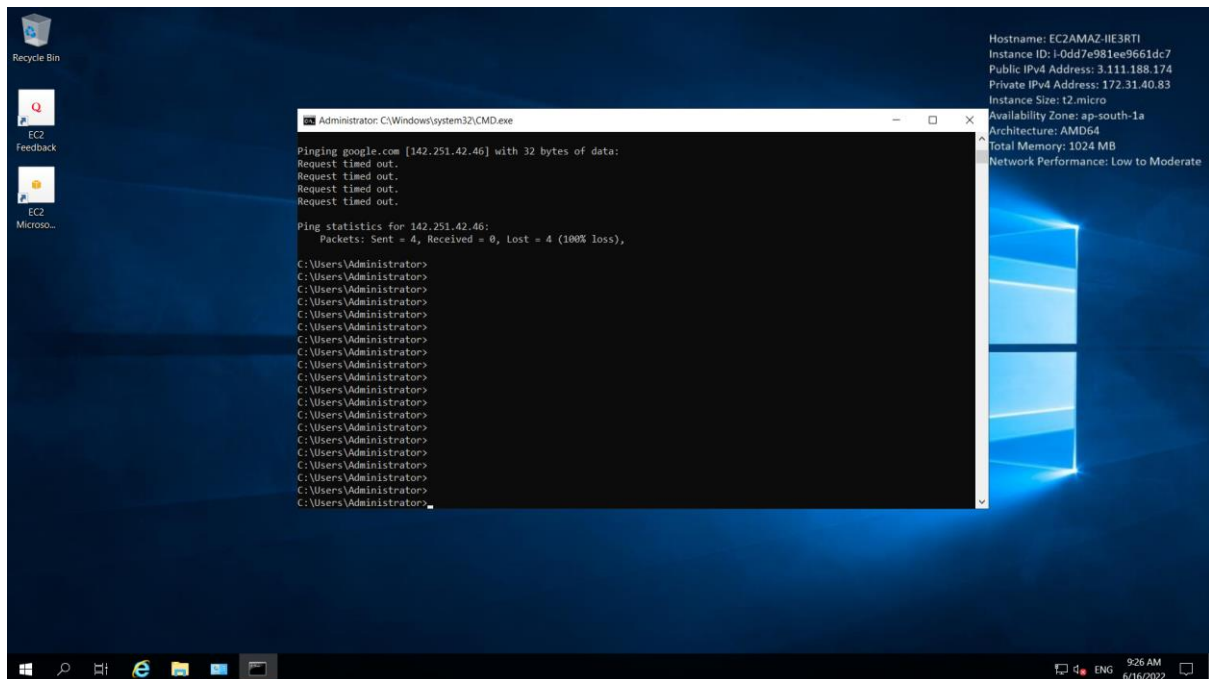
Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
10	RDP (3389)	TCP (6)	3389	0.0.0.0/0	Allow
100	All traffic	All	All	0.0.0.0/0	Deny

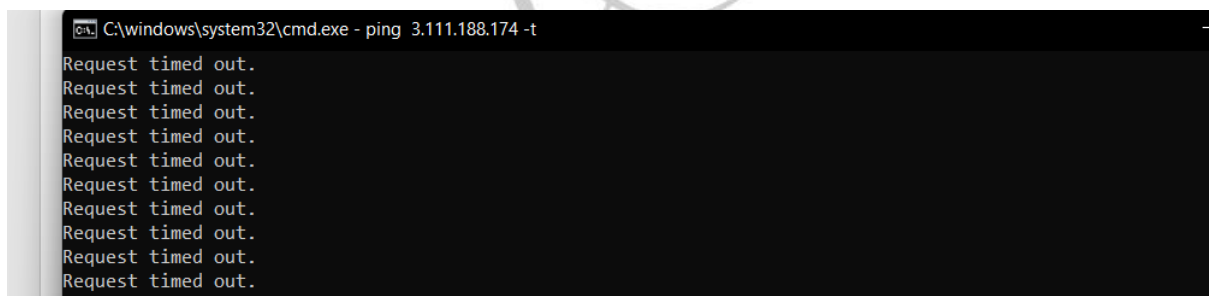
Difference between NACL vs SG

Now see whether you are able to ping to windows instance from your system or not or connect RDP

ONLY CONNECT RDP BECAUSE BOTH SIDE ONLY ENTRY RDP OR BLOCK (PING TO INSTANCE AND GOOGLE)



BLOCK PING LOCAL SYSTEM TO WINDOWS INSTANCE



IF INBOUND RULE: - ALL TRAFFIC ALLOW & OUTBOUND RULE: - ICMP IVP4 ALLOW

RESULT: - ONLY PING ALLOW LOCAL SYSTEM TO WINDOW INSTANCE BLOCK RDP & OTHER SERVICES