INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

Fundamentals of Aws Security Groups and NACL

Reena Hooda[1], Dr. Shivani[2]

[1]Assistant Professor, Department of CSE, Indira Gandhi University Meerpur, Rewari, Haryana, India

[2]Faculty, Department of CSE, Indira Gandhi University Meerpur, Rewari, Haryana, India

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1407000078

Abstract: AWS Security Groups and NACL, namely Network Access Control List act as a safeguard to protect the network and manage the incoming and outgoing data flow say traffic or data stream based on the specified rules and allow only authorized users to access the resources. There is a basic variance between security groups and NACLs in that security groups are actually a virtual firewall for EC2 instances, whereas NACLs work for subnets. The chapter highlights the security groups & NACL working, limitations and significance of integrating both.

Keywords: Security Groups, NACL, Cloud, Rules, Traffic.

I. Introduction

In today's digital age, cybersecurity has emerged as a crucial component for many businesses doing business through online resources like cloud computing. Cloud computing means storing, accessing and managing data as well as codes or programs on remote servers, say 'cloud' where data is hosted over the internet instead of the computer's local data center or hard disk. It is also referred to as Internet-based computing that allows management of the resources on the cloud and helps in concentrating on the development work that the company wants to do, rather than infrastructure, computation, storage, security, or privacy requirements or resource management. One of the important elements of cybersecurity is access control, and making sure only authorized people can access the business-critical data and utilize the resources. [1]

AWS Amazon Web Services provides the business a secure cloud compute platform and provides a scalable, secure and flexible environment that provides safety to data and also meets compliance requirements [4] [6] and offers a strong infrastructure where the business can manage its resources and build applications. There is a range of AWS services that can be utilized on a tenant basis. The huge infrastructure and vast range of secure services make AWS very popular for businesses interested in automating their work. Amazon Web Services is a secure, 24/7 available infrastructure that ensures the integrity and confidentiality of data and a platform to automate the various tasks where the designers can concentrate on their creative works. AWS offers security checks where the incoming and outgoing data can be controlled with rules and protocols. The security groups worked in a layered AWS architecture on a global infrastructure to protect privacy with sophisticated technical and physical measures to hinder unauthorized access. You will build on the most secure global infrastructure. To support regulatory compliance, AWS allows you to continually monitor the data and meet the various regulatory and compliance standards for finance, retail, healthcare, government etc. [1] The management of the access control in the cloud is done using the security groups offered by AWS. [4] The security groups work as a 'virtual firewall or virtual shields or protectors' to control the incoming and the outgoing traffic from 'Amazon EC2 (Amazon Elastic Compute Cloud)" instances, RDS (relational database service) instances, and other AWS services. [5] In an AWS VPC (virtual private cloud), rules specify the types of traffic that can access the resources. The outbound rules regulate the outgoing traffic. EC2 is a flexible and scalable computation service. [1] [8]

Steps to Create a Security Group

First, we have to visit the EC2 dashboard. After logging into AWS. Then select the security group in the EC2 dashboard. When we click the security group in the EC2 dashboard, a pop-up window appears where we have to select or click the Create Security Group button on the top side of the window in which we have to enter the security group name and also the description. After that we have to select the Virtual Private Cloud (VPC) along with the security group name, and description. Two other buttons are also there, named with Inbound and Outbound, which mention the rules. The inbound rules are created to enable access to the resources and allow traffic from certain IP addresses, ports etc. The outbound rules are used to manage the traffic that is permitted to depart from the resources. The new rules can also be created under inbound rules as well as outbound rules. Protocols, the port range, and destination IP addresses can also be used to build the rules, and then click on the Create button. [1][5][8]

Importance of AWS Security Groups

AWS Security Groups play a crucial role in ensuring the network security and protection of cloud data within the AWS infrastructure. They function like a strong shield, a virtual firewall, regulating the flow of incoming and outgoing traffic arriving at and departing from AWS resources. Each AWS resource, such as Amazon EC2 instances can be linked to one or many security groups. Each security group functions at the instance level to detect permitted traffic to reach the associated resources. These rules apply to both incoming and outgoing traffic and play a crucial role in the AWS ecosystem by acting as a watchman for both incoming and outgoing network traffic. These rules are predefined to determine whether the traffic should be allowed or denied. When a packet arrives at an AWS resource, the associated security group evaluates the defined rules. If the packet matches any of the rules that allow the traffic, it is permitted; otherwise, it is denied. Similarly, for outgoing traffic data flow is managed. AWS also offers multiple security groups for a single resource. By combining the rules of these security groups, AWS ensures flexibility

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

and easy management. [4] The evaluation of these rules follows principles of 'union, deny overrides allow and default deny' to allow or deny the traffic. [1]

Categories of AWS Security Groups

AWS Security Groups can be classified into two types based on their usage and functionality - these are [1] [5] [7]:

- EC2-Classic Security Groups: These security groups are specifically designed for instances that are launched in the traditional EC2-Classic network model and AWS recommends utilizing the Virtual Private Cloud (VPC) for new instances. By adopting VPC, users can hold more advanced networking capabilities.
- Virtual Private Cloud (VPC Security Groups): These security groups are designed for instances launched within a Virtual Private Cloud (VPC). VPCs provide enhanced networking features and are considered the standard method for creating separate network environments in AWS.

Limitations of Security Groups

In the security groups, an IP address cannot be blocked explicitly because it has any 'deny' rule. Further, there is a limit on the maximum number of incoming and outgoing traffic rules. The customer has to go for the service request to extend the security limit beyond 10,000. Another barrier is that it is also not able to stop the DNS traffic or the traffic received from the 'Route 53' which is an extremely accessible cloud domain name system to direct the end users to destined Internet applications by transforming names like aws.amazon.com into its numeric IP addresses that computers use for linking to other devices or modules. 'Amazon Route 53' cannot be used to connect the company's local networks with the AWS cloud. When a user enters the domain name, Route53 helps the user connect to that website, and if a failure is detected in connecting to that website, it automatically routes the user to a healthy link or the resource. Security groups cannot be requested for multiple 'Virtual Private Cloud' (VPC). [1] [7]

Deletion of Security Groups

To remove a security group using the AWS Management Console, users need to go to the EC2 Dashboard and choose the specific security group required to be deleted. Before deleting it, verify if associated instances are associated and disassociate them if required. Then click on the "actions" button and select the option "delete security group". After confirming the deletion, a deletion message will be received stating that the security group has been successfully removed. [7]

Network Access Control List (NACL)

Likewise security groups, Network access control list (NACL), too, is a 'virtual firewall' that functions [6] for subnets to control the incoming and outgoing data flow called traffic or the data stream of subnets. After the design of a VPC (virtual private cloud), automatically, a default NACL will be automatically linked that allows all incoming and outgoing traffic from anywhere. However, users can also customize NACL rules if required. If an explicitly defined rule is not found, then a default rule becomes actively linked automatically. Like the security groups, NACL also contains a set of rules for incoming and outgoing traffic to permit or reject it from the subnets. In NACL, users have both the options to allow traffic as well as to deny it.

AWS applies rule numbers to each rule. The major difference between security groups and is NACLs is that NACL works at the subnet level and security groups work for EC2 instances and other services like RDS. For instance, there are 2 subnets in a virtual private cloud, and if a user wants to give access to only the resources belonging to the second subnet. This will be implemented in NACL rather than Security Groups. Only authorized user will be given access to that second subnet and permitted to use its resources after verifying their IP address. Unlike the security groups, NACLs have an additional advantage that they can be associated with several subnets. However, a subnet can only be connected to a single NACL. [1] [3] association with a NACL, if a user tries to associate again, then the previous association is detached automatically, as NACLs are stateless, which means the information about old traffic is not remembered or kept. Fundamental notions in NACL are the rule number used for priorities, protocols, ports, source, and destination, the type of traffic, and permit or reject the traffic. [1] [2] [5]

Limitations of NACL

Like the security groups, **Network Access Control List (**NACL) rules are also limited, though more than security groups. The maximum NACL per virtual cloud is also limited, and moreover, a subnet can be associated with a single NACL at the same time. Further, NACL never keeps track of network connections in a subnet. [1]

Combining Security Group and NACL

Security group controls the incoming and outgoing traffic of an EC2 instance, and NACL is used for controlling the traffic at the subnet level is deployed in the virtual private clouds. Now combining both, EC2 instances will be installed in the VPC in a specific subnet. When there is incoming data flow, first, this flow must be checked by the NACL layer; after passing the NACL or being allowed by the NACL, it will be directed to security groups. If the data traffic is passed at both layers, it will be allowed to access the application, otherwise, it will not reach that application. NACL is most suitable for incoming traffic, and the security group is more suitable for outgoing traffic. A newly created NACL and Security group denies all inbound flow by default. The security

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

groups are stateful and provide the first layer of the security whereas the NACLs are stateless and work through explicitly defined rules, number for priorities and provide a second layer of the security [1] [7]

II. Conclusions

Security Groups operate at the 'instance level' in a Virtual Private Cloud (VPC), applying rules across all instances within the same VPC. AWS Security Groups are necessary for safeguarding the network from unauthorized traffic to EC2 instances, and are stateful, whereas NACLs work at the subnet level and are stateless and evaluate rules on a priority basis. Merging both provides additional security to the network and permits only the authorized traffic that is most necessary. Security Groups and NACLs empower effective traffic control and management of the best security practices within your AWS environment, protecting resources by offering an additional shield from unauthorized access and ensuring robust security mechanisms with flexibility in prioritized allow/deny rules.

References

1. What is a Security Group in AWS, and how to create it? - GeeksforGeeks
2. Bing Videos -Amazon Web Services – Security Group, https://youtu.be/_2HFqANE4gw?si=p_HPm-uKO4iOSI5a
3. Becki Lee (September, 2019). "Cloud Network Security 101: AWS Security Groups vs NACLs". Retrieved from: Cloud Network Security 101: AWS Security Groups vs NACLs (fugue.co)
4. Security and compliance - Overview of Amazon Web Services
5. AWS Security Groups: What They Are and How to Create Them (sentra.io)
6. AWS Security, Identity, and Compliance category icon Security, identity, and compliance - Overview of Amazon Web Services
7. Amazon Web Services - Security Group vs NACL - GeeksforGeeks
8. AWS Security Group - Javatpoint