Prevent Network-Related Attacks with Load Balancing in Cloud Services Providers

Ametovi Koffi Jacques Olivier[a], Ghufran Ahmad Khan ,[*], Taushif Anwar[a], Jalaluddin Khan[a], and Zubair Ashraf[b]

[a] Department of Computer Science & Application, Koneru Lakshmaiah Education Foundation Vaddeswaram, Andhra Pradesh, 522502, India.

[b]Department of Computer Engineering and Applications, GLA University, Uttar Pradesh, Mathura 281406, India.

Abstract. The Cloud refers to the provision of computing resources over the Internet in an on-demand manner, allowing for the storage, processing, and distribution of data. it helps to run applications and software through interconnected computer networks that provide services to individuals and organizations. The use of cloud services is growing exponentially, which gives rise to hackers who scan and analyze potential network vulnerabilities in the cloud architecture daily. To focus on the above-mentioned issue, we propose a novel idea to prevent large-scale DDoS attacks on the cloud through the adaption of load-balancing technology. To fulfill this task, we establish a virtual network with enabled Bastion service and DDoS protection. Further, it generates a standard SKU public load balancer, including a front-end IP address, integrity probe, back-end configuration, and load balancing rule. Afterward, the virtual machine is set up, and simulation is conducted through the attack on the network, which is described in the experiment section.

Keywords: Cloud, Load balancing, vulnerability, DDoS Attack; Protection Plan;

1. Introduction

Cloud computing (CC) is a rapidly advancing technology that has a significant influence on the real world. It offers a diverse array of applications in different industries [4]. CC has permeated nearly every facet of life, encompassing both social and professional growth. It entails network computations executed through cloud-based software applications, which are hosted on servers distributed throughout the Internet and can be accessed via browsers on mobile devices, desktops, laptops, and tablets.

Its modern, innovative technological trend enables companies to conquer the market by increasing their productivity, while helping to achieve objectives and also increase return on investment. Nowadays, many companies opt to utilize the services offered by the Cloud instead of constructing their own infrastructures, such as storing large datasets and eliminating administrative costs, while being accessible from anywhere which requires good organization and the distribution of workload traffic across several servers. In this scenario, the concept of load balancing is introduced which is located between the servers in the background and the devices used by clients. Whenever a request is received, the load balancer shares it among available servers using an algorithm like Round Robin or Weighted Round Robin that considers various criteria like server load and geographical distance.

The Cloud undoubtedly brings immense advantages, but security and confidentiality concerns are prevalent and act as major obstacles to its progress [4] [13]. Even though saving a company's

[*]Corresponding author. E-mail: editorial@iospress.nl. Check if the checkbox in menu *Tools/Options/Compatibility/Lay out footnotes like Word 6.x/95/97* is selected if you make a footnote for the corresponding author.

workloads on a publicly hosted cloud service offers significant benefits, it also exposes 94% of organizations to new data security risks. The primary cause is misconfiguration (68%), followed by illicit access (58%), vulnerable interfaces (52%), and phishing (50%), which are concerns shared by IT departments and customers alike [5].

According to a recent report from Aqua Security, the most common type of attack on cloud systems is Denial-of-Service Attacks (DoS).The threat of cyber-attacks looms large in the digital realm, making it essential to fortify your computer or network resource against potential breaches. These attacks have a singular objective: to render your system inaccessible to its intended users. A common technique employed by attackers is the Denial of Service (DoS) attack, which involves inundating a cloud service with an excessive volume of traffic. This flood of data overwhelms. The impact of cyber-attacks can be devastating, leading to significant disruptions, financial setbacks, and reputational damage for organizations. When it comes to defending against cloud-based Denial of Service (DoS) attacks, the challenges are even greater. Faced with the consequences that a DOS attack can cause then we expect to show in our research how to use load balancing to mitigate network-related attacks specifically DDOS attacks. This is the main motivational point for proposing this study, which will help cloud computing users to solve the security problem associated with DDOS attacks by making good configurations to their Microsoft Azure cloud services providers.

The article is structured as follows: Section 2 provides an overview of load-balancing algorithms and the vulnerabilities associated with cloud computing service providers. In Section 3, we delve into the concept of load balancing and its role within a cloud environment. Section 4 outlines the implementation of load balancing to mitigate DDOS attacks specifically in Microsoft Azure Cloud. Finally, Section 5 concludes the article.

2. Related work

In this section, we will give an overview of cloud service model, and load balancing.

2.1. Cloud Services

The concept of "cloud computing" pertains to the provision of storage, processing, analysis, and other data services through the internet, eliminating the need for local hardware. Businesses handle their IT operations by connecting to a service provider and utilizing third-party services. Cloud services can be categorized based on their business model, functionality, and billing system. Now, let's examine the features and

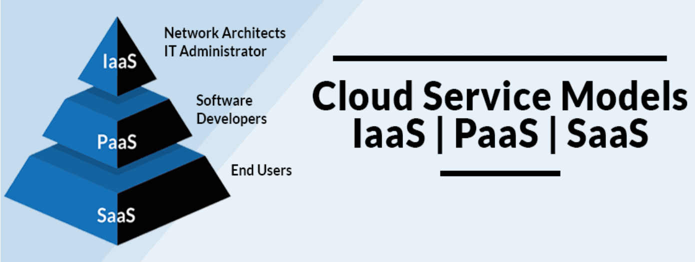


Fig. 1. Different cloud services.

2.1.1. Infrastructure as a Service (IaaS)

IaaS is an internet-based computer infrastructure that is managed online. One of the main advantages of using IaaS is that it allows consumers to save money and avoid the inconvenience of purchasing and managing physical servers [1]

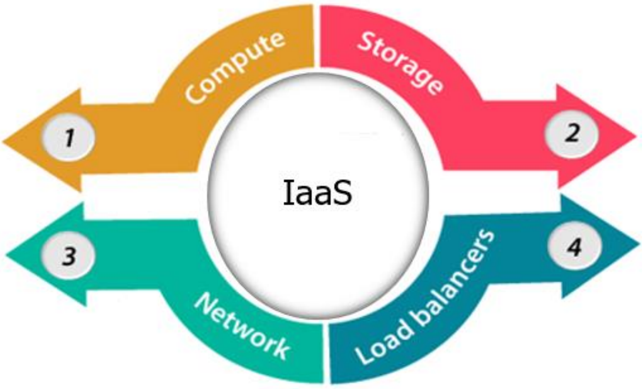


Fig. 2. IaaS Characteristics.

Here are a few examples of IaaS providers: Google, Microsoft Azure, IBM Smart Cloud, Linode, and Digital Ocean [19.]

2.1.2. Platform as a Service (PaaS)

For programmers, the PaaS cloud computing platform was specifically designed to facilitate the creation, testing, execution, and management of applications [17]. Fig. (3) Highlights its significant characteristics. Some well-known PaaS include SAP Cloud, Apprenda Cloud, Kinsta, and Cloudways [15].

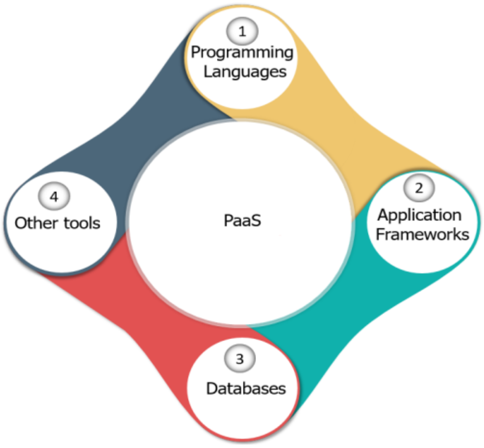


Fig. 3. PaaS Characteristics

2.1.3. Software as a Service (SaaS)

SaaS is a cloud-hosted software solution. Users can access these applications via a browser and a connected network. Photopea, Concur, DocuSign, and GoToMeeting are just a few popular examples of SaaS. The main characteristics of SaaS are illustrated in Fig. (4).

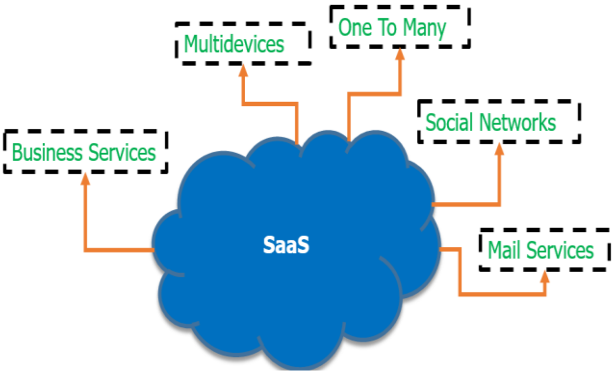


Fig. 4. SaaS Characteristics

As the availability of cloud services increases, so do their applications in the corporate world. These services will continue to simplify the way organizations deliver critical applications and data to their people, whether the company chooses to extend existing on-premise software deployments or migrate 100% to the cloud. Cloud services (IaaS, PaaS and SaaS) are transforming the way people work and the way businesses operate, from application delivery to desktop virtualization solutions, including a wide range of features such as load balancers.

2.2. Load balancing

Over the past decade, online traffic has experienced exponential growth. Web users are demanding improved access speed and security, resulting in high demand for web servers. Load balancing was employed as a workload optimization strategy. Load balancing ensures a server cluster can manage peak traffic and supply backup solutions during outages. This is where the load balancer becomes instrumental. The workload is balanced between servers to maintain their capacity at an optimal level [10]. Cloud-based load-balancing services are commonly used to distribute traffic across multiple servers and ensure high availability and performance for web applications as shown in Fig. (5) Below.

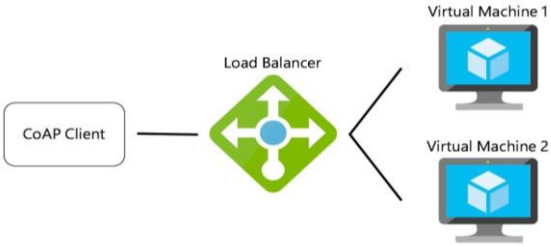


Fig. 5. Example of Load Balancing

A load balancer (LB) is an essential element of the IaaS, as shown in Fig. (2). It requires a dedicated infrastructure. Instead of investing in expensive hardware with a server acting as the LB, the LB software can be installed on a VM (Virtual Machine) which acts as the ADC [21].

This installation results in an ADC. Virtual LBs offer greater flexibility and enable automatic scaling based on traffic forecasts. They dynamically select the best server to handle a request, ensuring a constant level of performance for the cluster. In the event of a hardware failure, when a user requests a web page, the LB redirects the workload to another server [10], [14].

2.2.1. Load balancing in the cloud

Load balancing in the cloud can refer to two distinct concepts: balancing workloads that are hosted in the cloud or utilizing load balancers that are specifically designed for cloud environments. In a cloud computing environment, load balancing involves managing the traffic associated with a company's cloud-based workloads and distributing it across multiple resources, such as server groups and networks [9]. The significance of load balancing in the cloud is on par with other scenarios, as it aims to achieve high availability and optimal performance. By evenly distributing the traffic, workload performance is enhanced, and the likelihood of system outages is minimized [23].

Cloud-based load balancers, available in a pay-as-you-go model, offer exceptional elasticity and flexibility. They provide various functionalities, including health checks and controlled resource access. However, the effectiveness of these load balancers may vary depending on the vendor and the specific environment in which they are deployed. To optimize traffic distribution and improve resource performance, cloud-based load balancers can utilize algorithms such as round robin, weighted round robin, and least connections [20].

Cloud-based load balancing services have the advantage of being simple to set up and use. There is no need to install, configure, or maintain load-balancing hardware or software, as the provider manages all the details. Additionally, you can make use of the cloud provider's knowledge and proficiency in load balancing, while benefiting from their regular updates and improvements. Another advantage of cloud-based load-balancing services is their scalability and flexibility. You can effortlessly add or remove servers from the server pool and adjust the load-balancing parameters and rules to suit your needs and preferences. Furthermore, you can capitalize on the provider's global network and infrastructure to distribute your traffic over several regions and zones [14], [20], [21].

A potentially chaotic situation in the cloud is brought under control by load balancing, which acts as a "traffic cop"[31]. Load balancing also enables controls, such as virtual infrastructures and applications, to be carried out to guarantee availability and avoid downtime due to problems. Even more manageable centralized security can be provided by load-balancing the entire server cluster. The potential of load balancing to act as a "traffic cop” will be the subject of the next section.

2.2.2. Load Balancing Algorithms

Load balancers use algorithms or mathematical formulae to determine which server should handle each request as part of load balancing. The traffic routing is evaluated differently by various algorithms, depending on whether it is at the network or application layer. There are two main groups of load-balancing algorithms: weighted and non-weighted. Weighted algorithms make decisions based on weights or preferences, ensuring that servers with higher weights receive a greater share of traffic. These algorithms take into account both the individual server weights and the total weight of all servers in the group [31]. Non-weighted algorithms do not distinguish between servers since they assume that they all have the same capacity. This method expedites load balancing but ignores the fact that different servers have different capacities [22], [27].

2.2.3. Load Balancing Methods

Load balancing methods are dependent on specific criteria to determine which server in a server farm should receive the next request. There are five commonly utilized load balancing methods:

- The default method is Round Robin, where requests are directed in a rotating fashion. Each server in the group handles requests in a sequential manner, ensuring an equitable distribution of connections [21], [24].

- In Weighted Round Robin, servers are given weights according to their capacity, resulting in servers with higher weights being allocated a higher number of requests compared to servers with lower weights [20],[23].

- Sticky sessions, establishes a link between clients and servers throughout a session. To maintain consistency, the load distribution relies on a user attribute, such as a cookie or IP address, to guarantee that every request coming from a specific user are systematically sent to a dedicated server until the session is completed [28],[29],[30].

Remember, these are just a few of proper load distribution methods available, each serving different purposes and catering to specific needs.

3. Implement load balancing to mitigate DDOS attacks in Microsoft Azure Cloud

In the previous section, we looked at the role of the load balancing in a cloud environment and the many algorithms that can be used to address current cloud security concerns. To reduce DDOS attacks, cloud service providers such as Microsoft Azure, AWS, and IBM have created a variety of strategies, such as load balancing configurations in cloud spaces.

In this part, we'll talk about Azure DDoS Protection, which provides enhanced DDoS mitigation features including adaptive setting, attack alerts, and surveillance to safeguard your public charge balancers from massive DDoS attacks.

3.1. Create a DDoS protection strategy

Before starting to create a DDOS protection policy, you need to create an Azure account with an active subscription. Once the account has been created, enter Identity Access Management (IAM) in the Azure Portal to access the dashboard shown in Fig. (6). the following information must be entered or selected on the Basics tab of the Create DDoS Protection Plan page:

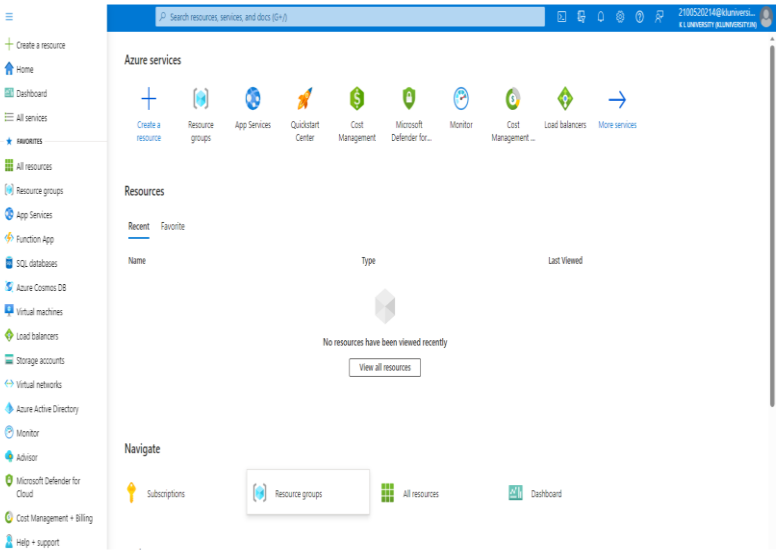


Fig. 6. Azure Portal Dashboard.

Project details:

- Subscription: azure for students
- Resource group: ****

  Select Create new

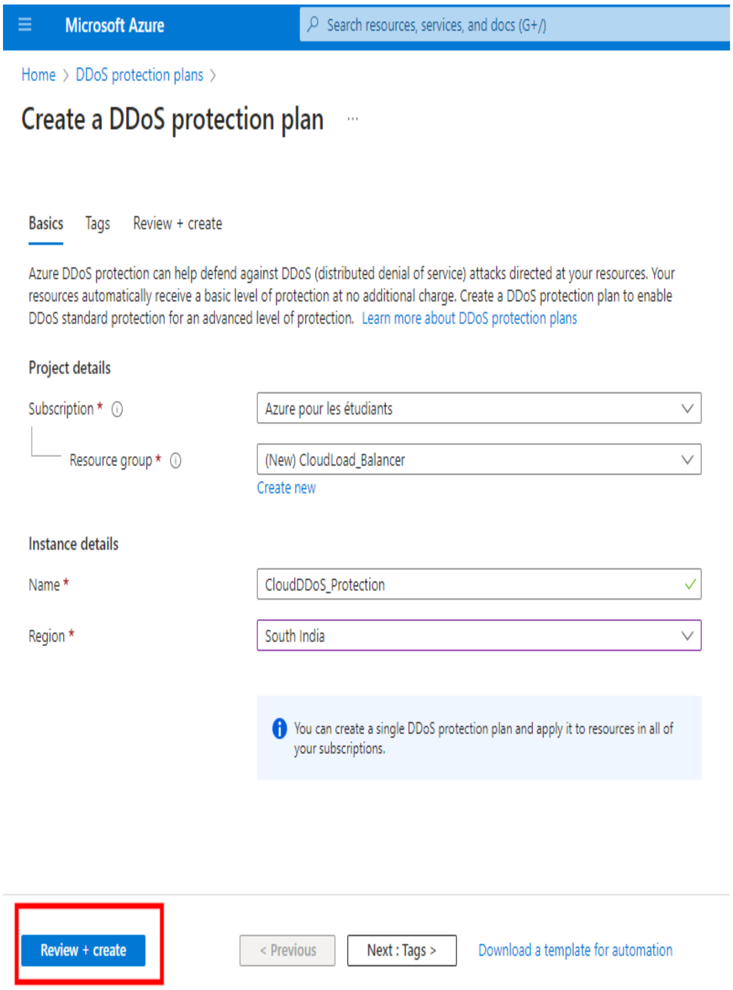
  Name: ****

  Select OK.

Instance details:

- Name: ****
- Region: ****

Afterward, select Review + Create, then click create to deploy the DDoS protection plan as shown in Fig. (7).



Microsoft Azure

Search resources, services, and docs (G+/)

Home > DDoS protection plans >

Create a DDoS protection plan

Basics | Tags | Review + create

Azure DDoS protection can help defend against DDoS (distributed denial of service) attacks directed at your resources. Your resources automatically receive a basic level of protection at no additional charge. Create a DDoS protection plan to enable DDoS standard protection for an advanced level of protection. Learn more about DDoS protection plans

Project details

Subscription *	Azure pour les étudiants
Resource group *	(New) CloudLoad_Balancer Create new

Instance details

Name *	CloudDDoS_Protection
Region *	South India

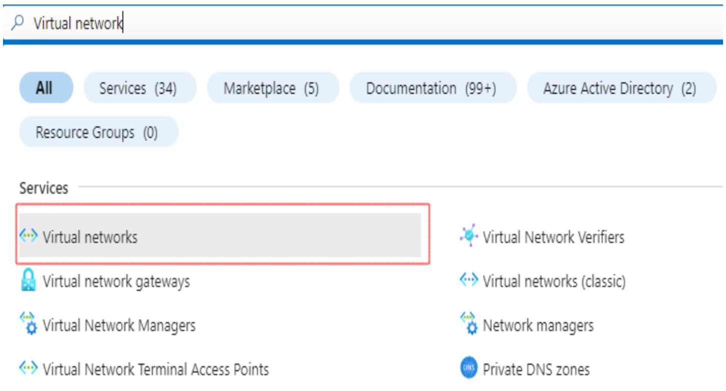
You can create a single DDoS protection plan and apply it to resources in all of your subscriptions.

Fig. 7. Basics DDoS Protection

3.2. Create a virtual network

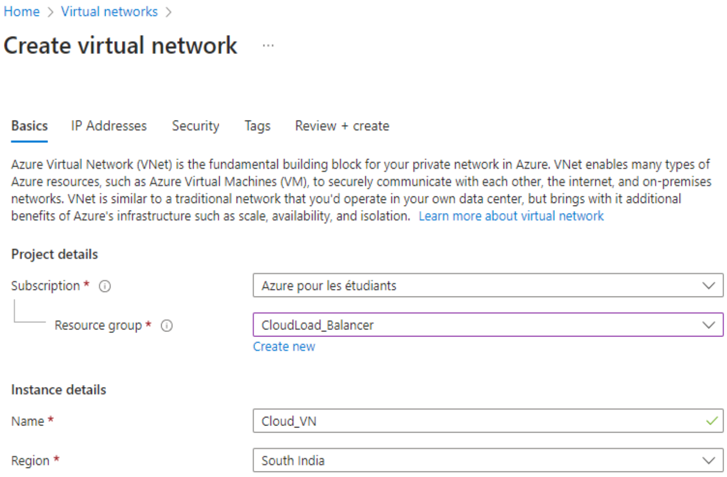
This section outlines the steps for establishing a virtual network, subnet, and Azure Bastion host and connecting them to the DDoS protection plan. Virtual networks and subnets comprise load balancers and virtual machines. The Bastion host is responsible for managing virtual machine security. The DDoS protection plan safeguards all public IP resources within the virtual network.

During the process of configuring the public IP address, a key aspect of its configuration will be the ability to enable or disable the DDoS protection plan previously created in the section 3.1 and located in the security tab, as this functionality is vital for conducting our tests and guaranteeing security reliability. All the steps required to create and configure a virtual network are illustrated in Figs. (8), (9), (10), (11) and (12).



Virtual network

Fig. 8. Virtual Networks.



Home > Virtual networks >

Create virtual network

Basics | IP Addresses | Security | Tags | Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. Learn more about virtual network

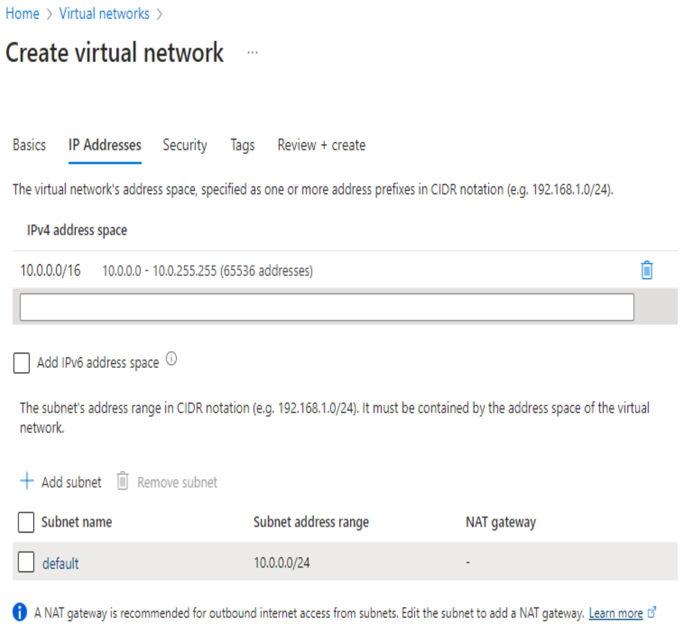
Project details

Subscription *	Azure pour les étudiants
Resource group *	CloudLoad_Balancer Create new

Instance details

Name *	Cloud_VN
Region *	South India

Fig. 9. Basics Virtual Networks.



Home > Virtual networks >

Create virtual network ···

Basics | **IP Addresses** | Security | Tags | Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space	
10.0.0.0/16	10.0.0.0 - 10.0.255.255 (65536 addresses)

□ Add IPv6 address space ⓘ

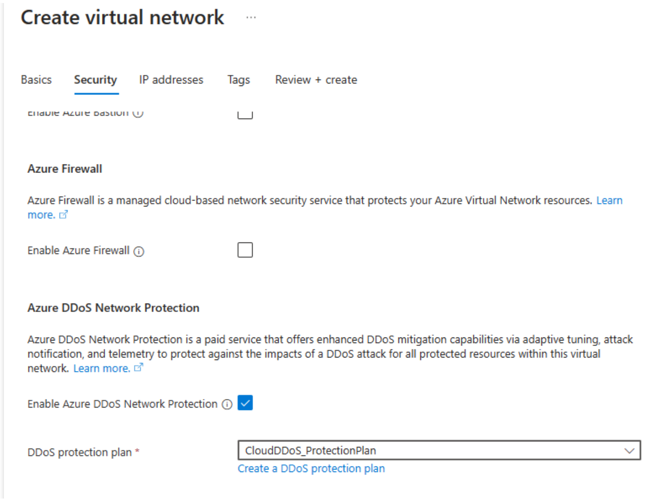
The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet   Remove subnet

□ Subnet name	Subnet address range	NAT gateway
□ default	10.0.0.0/24	-

ⓘ A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more

Fig. 10. IP Address configuration.



Create virtual network ···

Basics | **Security** | IP addresses | Tags | Review + create

Enable Azure Bastion ⓘ □

Azure Firewall

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. Learn more.

Enable Azure Firewall ⓘ □

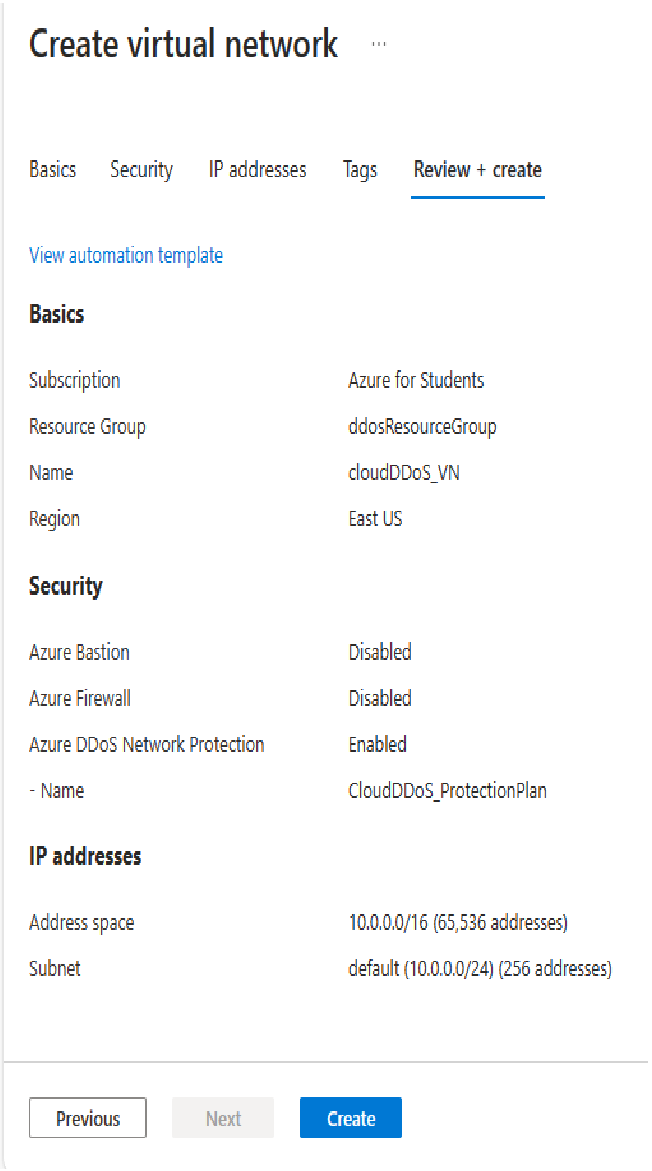
Azure DDoS Network Protection

Azure DDoS Network Protection is a paid service that offers enhanced DDoS mitigation capabilities via adaptive tuning, attack notification, and telemetry to protect against the impacts of a DDoS attack for all protected resources within this virtual network. Learn more.

Enable Azure DDoS Network Protection ⓘ ☑

DDoS protection plan * CloudDDoS_ProtectionPlan
Create a DDoS protection plan

Fig. 11. Tab Security for disable or enable DDoS Protection Plan



Create virtual network ···

Basics | Security | IP addresses | Tags | **Review + create**

View automation template

Basics

Subscription	Azure for Students
Resource Group	ddosResourceGroup
Name	cloudDDoS_VN
Region	East US

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Enabled
- Name	CloudDDoS_ProtectionPlan

IP addresses

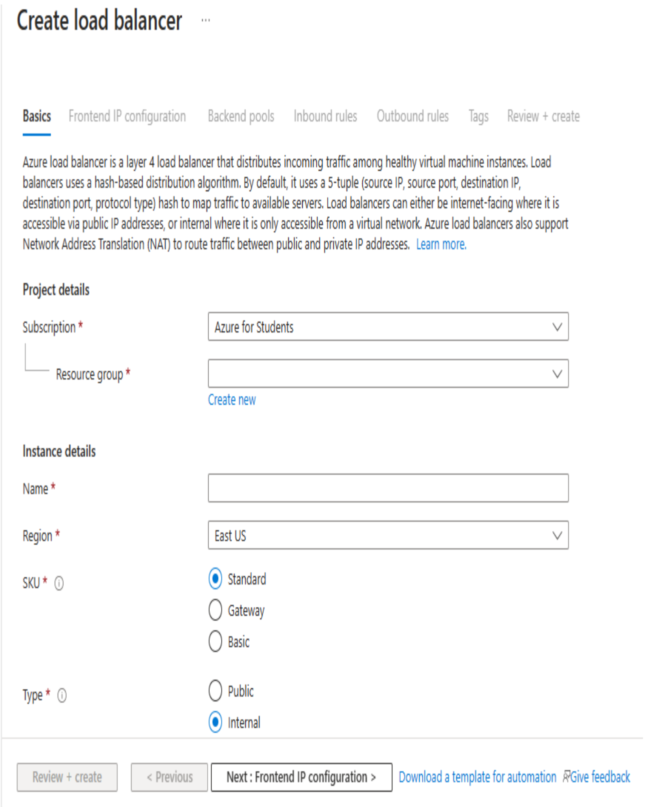
Address space	10.0.0.0/16 (65,536 addresses)
Subnet	default (10.0.0.0/24) (256 addresses)

Fig. 12. Overview of Create Virtual Network

3.3. Create a load balancer and a public IP address

To effectively distribute the workload among virtual machines and ensure uninterrupted communication between Azure resources and external Internet resources, we will implement redundant zone architecture to create a load balancer. This architecture guarantees that the data path remains intact, even if multiple availability zones fail, as long as at least one zone in the region remains operational. Additionally, we will establish a public IP address to facilitate this communication.

During the configuration process for the load balancer, we will set up the front-end IP address, back-end pool, incoming load balancing rules, and integrity probe. An overview of all the steps involved is shown in Fig. (13), and (14):



Create load balancer ···

Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers uses a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. Learn more.

Project details

Subscription * Azure for Students

Resource group *

Create new

Instance details

Name *

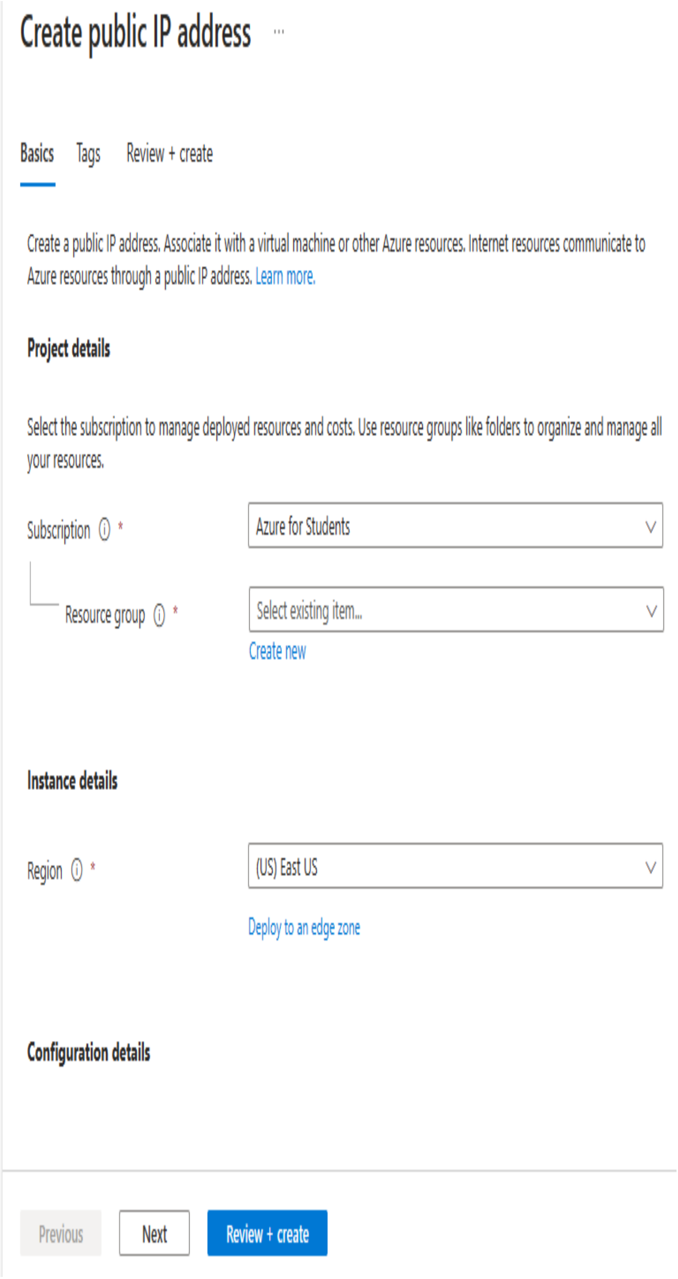
Region * East US

SKU * ● Standard ○ Gateway ○ Basic

Type * ○ Public ● Internal

Review + create
< Previous
Next : Frontend IP configuration >
Download a template for automation
Give feedback

Fig. 13. Basic configuration of load balancer creation.



Create public IP address ···

Create a public IP address. Associate it with a virtual machine or other Azure resources. Internet resources communicate to Azure resources through a public IP address. Learn more.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure for Students

Resource group * Select existing item...

Create new

Instance details

Region * (US) East US

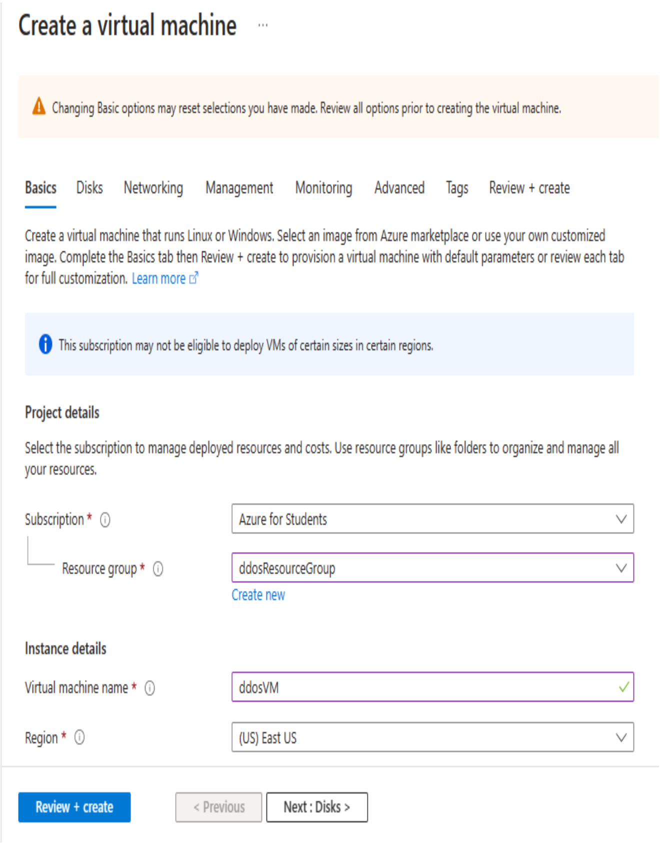
Deploy to an edge zone

Configuration details

Fig.14. Basic configurations of IP address creation.

3.4. Create Virtual Machines

This section is about creating a virtual machine and configuring it. The virtual machine will be associated with the load balancer backend pool and the public IP address created in the previous section 3.3 and shown in Fig. (15), (16), (17), and (18).



Create a virtual machine

⚠ Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

ⓘ This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

Project details

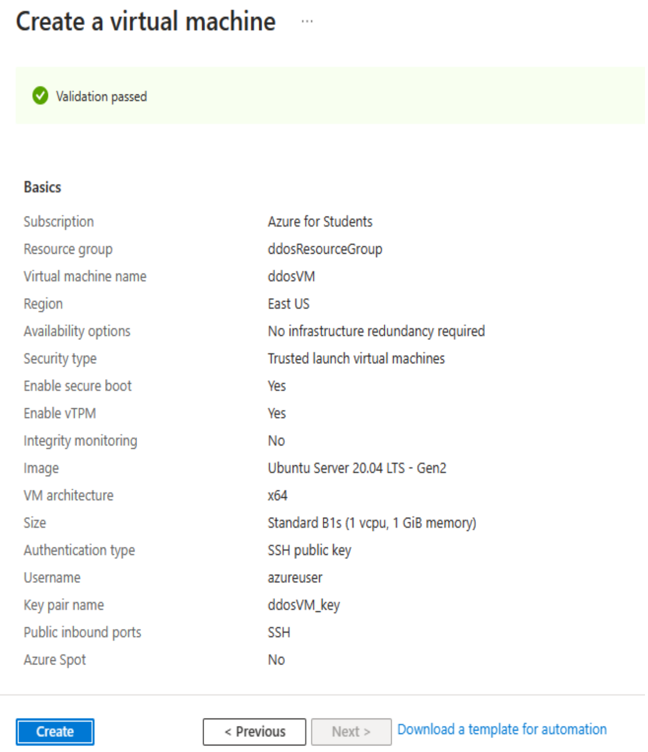
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Azure for Students
Resource group *	ddosResourceGroup Create new

Instance details

Virtual machine name *	ddosVM ✓
Region *	(US) East US

Fig. 15. Basic configuration of virtual machine creation.



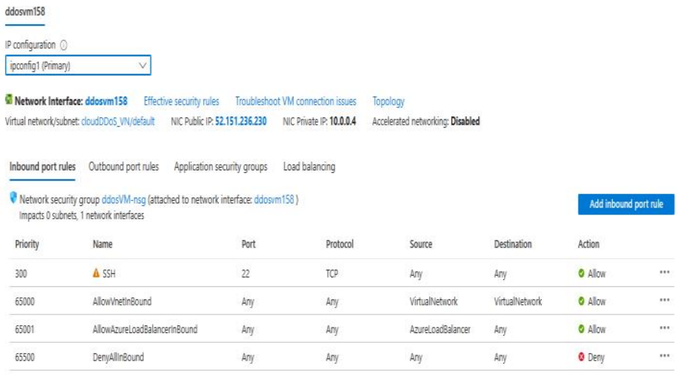
Create a virtual machine

✓ Validation passed

Basics

Subscription	Azure for Students
Resource group	ddosResourceGroup
Virtual machine name	ddosVM
Region	East US
Availability options	No infrastructure redundancy required
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Ubuntu Server 20.04 LTS - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GiB memory)
Authentication type	SSH public key
Username	azureuser
Key pair name	ddosVM_key
Public inbound ports	SSH
Azure Spot	No

Fig. 16. Overview of virtual machine creation.



ddosvm158

IP configuration ⓘ: ipconfig1 (Primary)

Network Interface: ddosvm158 Effective security rules Troubleshoot VM connection issues Topology

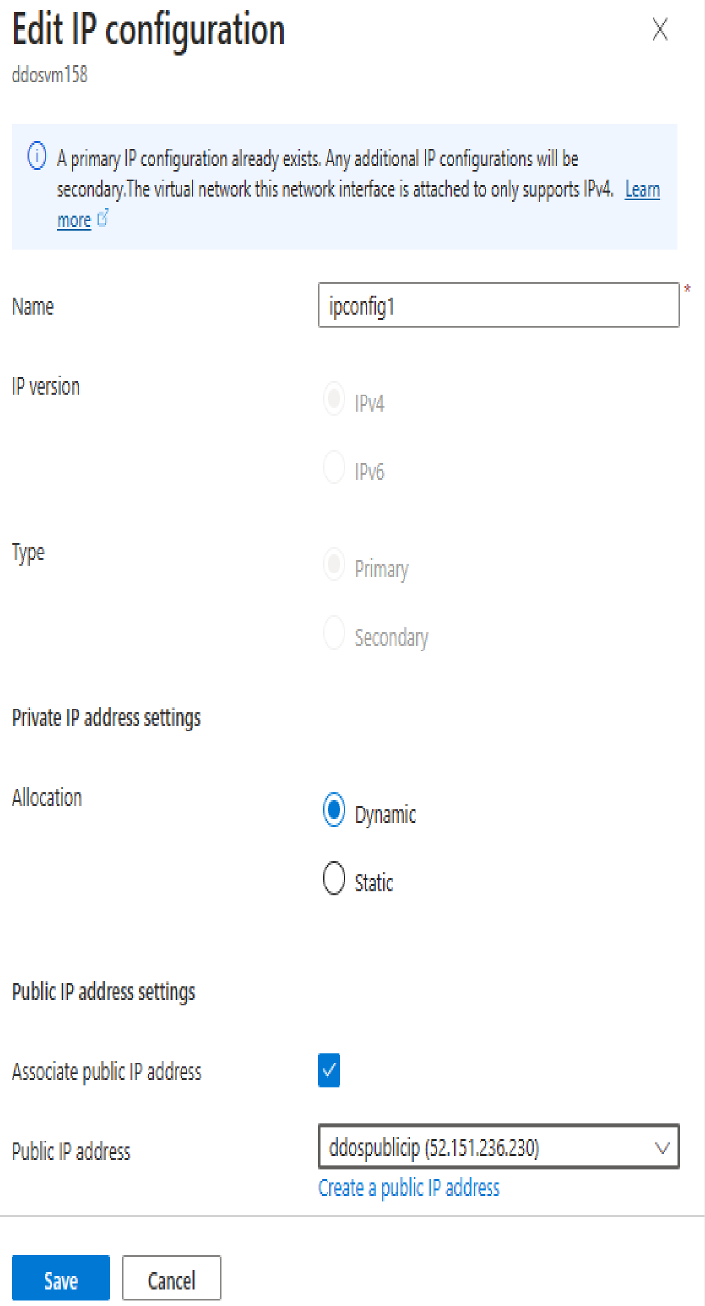
Virtual network/subnet: cloudDDoS_VN/default NIC Public IP: **52.151.236.230** NIC Private IP: **10.0.0.4** Accelerated networking: **Disabled**

Network security group ddosVM-nsg (attached to network interface: ddosvm158)
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
300	⚠ SSH	22	TCP	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

Fig. 17. Overview of virtual machine network.

5.



Edit IP configuration

ddosvm158

ⓘ A primary IP configuration already exists. Any additional IP configurations will be secondary.The virtual network this network interface is attached to only supports IPv4. Learn more

Name: ipconfig1 *

IP version: ○ IPv4 ○ IPv6

Type: ○ Primary ○ Secondary

Private IP address settings

Allocation: ● Dynamic ○ Static

Public IP address settings

Associate public IP address: ☑

Public IP address: ddospublicip (52.151.236.230)

Fig. 18. Edition of virtual machine

4. Experimental Analysis

This section outlines the simulation of a tenth DDoS attack on the Microsoft Azure environment to evaluate the effectiveness of the DDoS protection plan. The test will consist of two scenarios: scenario 1 will show the results of the DDoS stimulation test while the protection plan is disabled, and scenario 2 will show the results with the protection plan enabled. To do this, we will use IXIA BreakingPoint Cloud on Microsoft Azure, a cloud application testing and security platform powered by Keysight's ATI subscription service. BreakingPoint offers a variety of simulations for applications and attacks that replicate the traffic and security threats faced by enterprises, service providers, or government organizations of any size. Its comprehensive network stack includes components such as IPv4, IPv6, DNS, and DHCP, which enhance the application and attack simulations. The network components help to orchestrate the network environments required for the simulations. The purpose of these attack simulations is to evaluate the effectiveness of our DDoS protection plan, whether it is enabled or disabled.

To begin our stimulation tests, we must first create multiple accounts on the IXIA Breakpoint Cloud test space. Next, we need to create an alert rule that is linked to the parameter of our DDoS protection plan. Finally, we must configure the metrics in the monitoring parameters of our public IP address.

4.1. Scenario 1

On December 15, 2023, between 12:30 and 13:12 (UTC+05:30), our public IP address was subjected to three DDoS attacks at 10-minute intervals. The attack profile used was DNS Flood, with a size of 100,000 packets per second and 60 Mbps, originating from two source IP addresses. The results of the tests are presented below.

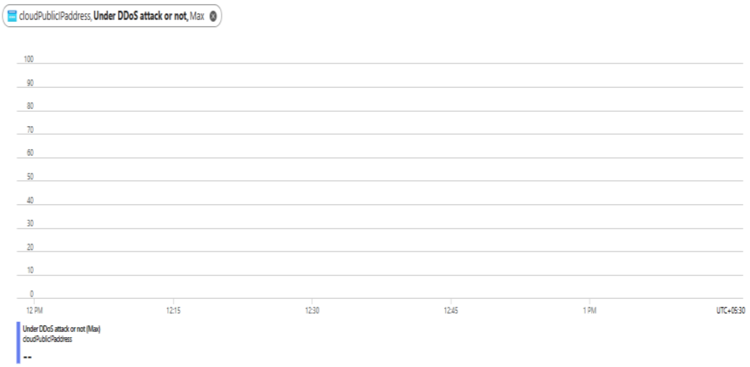


Fig. 19. Results metrics of scenario 1

Although the public IP address associated with our virtual machine was attacked, the maximum total value of the DDOS attack or not showed no value. At first glance, the normal traffic of the Azure Cloud server seems to be functioning properly, but this is not the case. Indirectly, the normal traffic was overwhelmed with an equivalent of 177,886,907 frames sent, resulting in a total outgoing data of 13520 Megabytes, which is 13.52 Gigabytes.

4.2. Scenario 2

During scenario 2, we enabled the DDoS protection plan and conducted tests that focused on 7 10-minute attacks using DNS Flood as the DDoS attack profile. The attack size was 100,000 pps and 60 Mbps, with two sources IPs. The tests were conducted on December 15, 2023, from 13:29 to 15:16 (UTC+05:30). The results are presented in various types of metrics charts below.

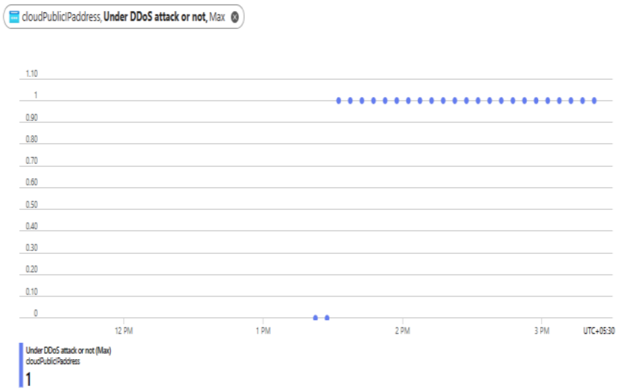


Fig. 20. Results Metrics in a Scatter Chart

The scatter format results display the DDoS protection plan's response to seven attacks. Each attack is represented by three successive points, indicating the attack's start and end times. The maximum aggregate value is 1, indicating DDoS attack. The two points located at value 0 represent the attack's initiation phase before reaching its maximum value, which remains constant until the last attack.

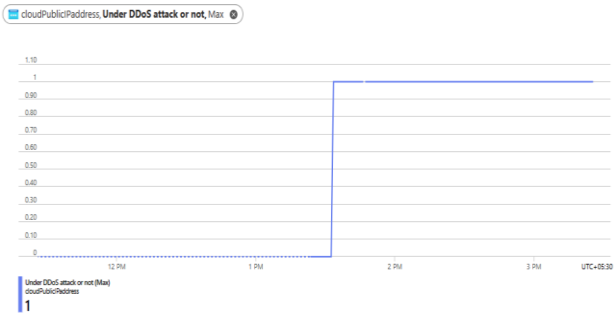


Fig. 21. Results Metrics in a Line Chart of scenario 2

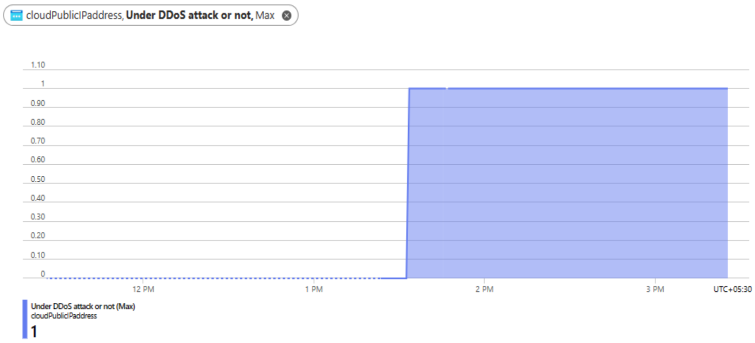


Fig. 22. Results Metrics in an Area Chart of scenario 2

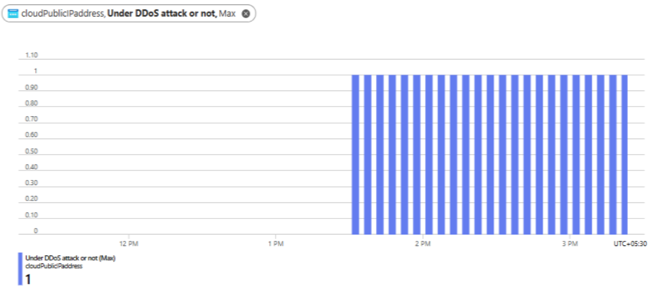


Fig. 23. Results Metrics in a Bar Chart of scenario 2

Fig. (21), (22) and (23) demonstrate that the max aggregate value at the start of the attack was zero. The value of the aggregate progressively increased at the beginning of the attacks, regardless of whether it was under DDoS attack or not, reaching its maximum value of 1 at the end of attack 4. This value remained constant during the following attacks, which explains the constant horizontal line until the end of the last attack.

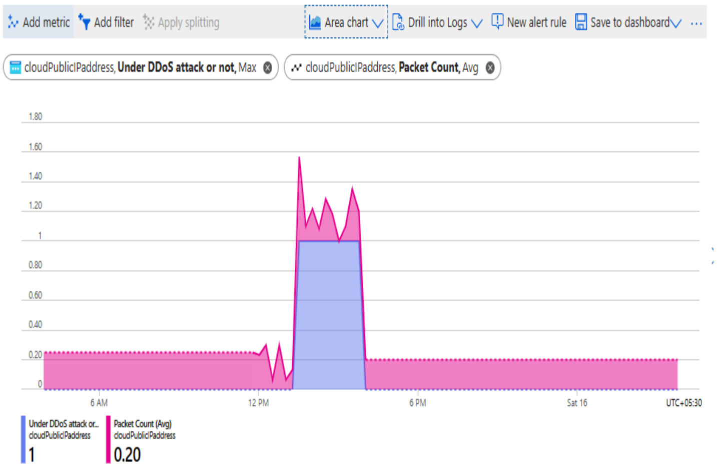


Fig. 24. Combination of Area Chart and Packet Count,

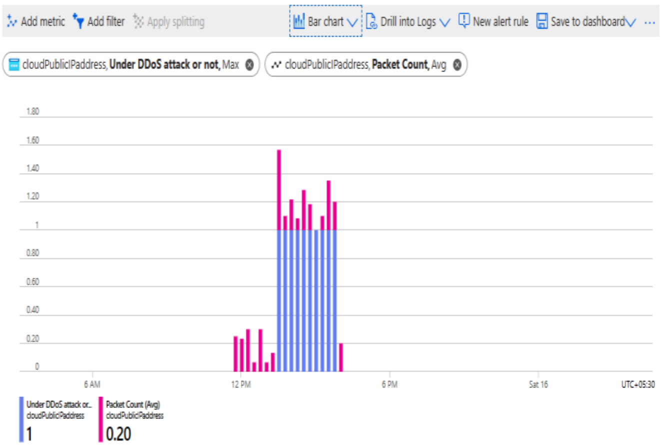


Fig. 25. Combination of Bar Chart and Packet Count, Avg.

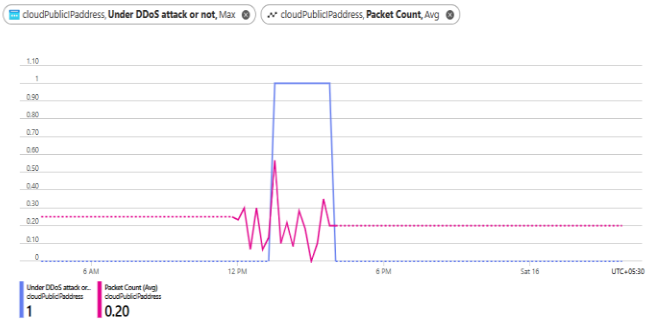


Fig. 26. Combination of Line Chart and Packet

Fig. (24), (25), and (26) display the average packet count, which is 0.20. This represents the total number of packets transmitted during the attack period.

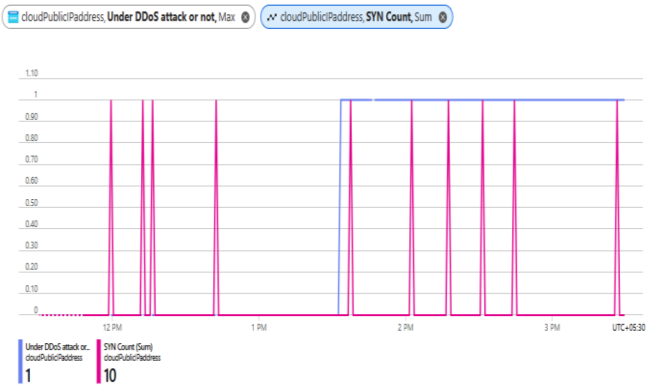


Fig. 27. Combination of Line Chart and SYN Count, Sum.

Fig. (27) Show the sum of the SYN Count, which is 10, representing the total number of SYN packets transmitted during the attack period. A SYN packet metric measures the number of TCP SYN packets received or sent by a load balancer front end. TCP SYN packets initiate a TCP connection between a source and a destination. This metric can aid in troubleshooting and understanding the volume and health of TCP connections.

6. Conclusion

This research addresses the vulnerability issue of cloud computing i.e. misconfiguration. To mitigate potential back and front-end cloud security attacks like Dos and DDoS, we executed a practical configuration phase on a Microsoft Azure account employing the load balancing concept. This study demonstrates how load balancing can mitigate the potential attacks generated by future attacks. It is worth mentioning that the suggested model in this study can also be implemented with other cloud service providers, including AWS, Oracle Cloud.

References

[1] Mosco, Vincent, 2016. After the internet: Cloud computing, big data and the internet of things. Les Enjeux de l'information et de la communication, (2), 146-155.

[2] AMIT SHEPS, 2024. Top 10 Cloud Attacks and What You Can Do About Them, (January).https://www.aquasec.com/cloud-native-academy/cloud-attacks/cloud-attacks/.(Accessed 5 October 2023).

[3] Elsa T, 2022. Cloud Security: Issues and challenges of security in the cloud, (January).https://www.cyberuniversity.com/post/la-securite-dans-le-cloud-principaux-risques-et-challenges. (Accessed 7 November 2023).

[4] OCloud Solutions, 2022. Impacts of Cloud Computing on Businesses, (May). https://www.linkedin.com/pulse/impacts-cloud-computing-businesses-ocloud-solutions.(Accessed 15 November 2023).

[5] Cyber-hub. Top 15 Cloud Security Issues: Threats and Concerns. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns. (Accessed 5 October 2023).

[6] Cloud Security Alliance (CSA), 2022. Cloud Security Alliance's Top Threats to Cloud Computing: Pandemic 11 Report Finds Traditional Cloud Security Issues Becoming Less Concerning, (June). https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning. (Accessed 5 October 2023).

[7] Holger Schulze, 2023. Cloud Security Report, Cybersecurity Insiders

[8] Joseph Bradley, James Macaulay, Andy Noronha, Hiten Sethi, 2013. The Impact of Cloud on IT Consumption Models, Intel-Cisco.

[9] Basetty Mallikarjuna, Arun Kumar Reddy Dodd, 2019. The Role of Load Balancing Algorithms in Next Generation of Cloud Computing, Journal of Advanced Research in Dynamical and Control Systems. Vol. 11, 07-Special Issue, 2019.

[10] Santosh T. Waghmode, Bankat M. Patil, 2023. Adaptive Load Balancing in Cloud Computing Environment, IJISAE, 11(1s), 209–217.

[11] Zhou, C.V., Leckie, C. and Karunasekera, S., 2010. A survey of coordinated attacks and collaborative intrusion detection. Computers & security, 29(1), pp.124-140.

[12] Kilari, N. and Sridaran, R., 2018. A novel approach to protect cloud environments against DDOS attacks. In Big Data Analytics: Proceedings of CSI 2015 (pp. 515-523). Springer Singapore

[13] Khan, Jalaluddin, Jian Ping Li, Bilal Ahamad, Shadma Parveen, Amin Ul Haq, Ghufran Ahmad Khan, and Arun Kumar Sangaiah. "SMSH: Secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption." IEEE Access 8 (2020): 15747-15767.

[14] Chaczko, Z., Mahadevan, V., Aslanzadeh, S. and Mcdermid, C., 2011, September. Availability and load balancing in cloud computing. In International conference on computer and software modeling, Singapore (Vol. 14, pp. 134-140). IACSIT Press.

[15] Chou, T.S., 2013. Security threats on cloud computing vulnerabilities. International Journal of Computer Science & Information Technology, 5(3), p.79.

[16] Robinson, R.J., 2023. Insights on Cloud Security Management. Cloud Computing and Data Science, pp.212-222.

[17] Fadhil, I.S.M., Nizar, N.B.M. and Rostam, R.J., 2023. Security and privacy issues in cloud computing. Authorea Preprints.

[18] Rashmi. R.Kamat, 2023. A Cloud Computing, International Journal of Scientific Research & Engineering Trends, Volume 9, Issue 2, 2395-566.

[19] Mahesh, K., Yaddanapudi, P. and Burugupalli, K., 2023. A Review of the Challenges and Opportunities in Cloud Computing Services.

[20] Joshi, V., 2019. Load Balancing Algorithms in Cloud Computing. International Journal of Research in Engineering and Innovation, 3, pp.530-532.

[21] Gupta, H. and Sanghwan, S., 2017. Load Balancing in cloud computing. International Journal of Recent Trends in Engineering and Research, 3(3), pp.260-267.

[22] Khan, J., Khan, G.A., Li, J.P., AlAjmi, M.F., Haq, A.U., Khan, S., Ahmad, N., Parveen, S., Shahid, M., Ahmad, S. and Raji, M., 2022. Secure smart healthcare monitoring in industrial internet of things (iiot) ecosystem with cosine function hybrid chaotic map encryption. Scientific Programming, 2022.

[23] Zaouch, A. and Benabbou, F., 2015. Load balancing for improved quality of service in the cloud. International Journal of Advanced Computer Science and Applications, 6(7), pp.184-189.

[24] Arian, T., Kusedghi, A., Raahemi, B. and Akbari, A., 2017. A Collaborative Load Balancer for Network Intrusion Detection in Cloud Environments. J. Comput., 12(1), pp.28-47.

[25] Shah, J.M., Kotecha, K., Pandya, S., Choksi, D.B. and Joshi, N., 2017, May. Load balancing in cloud computing: Methodological survey on different types of algorithm. In: 2017 International conference on trends in electronics and informatics (ICEI). IEEE, pp. 100-107.

[26] Heorhiadi, V., Reiter, M.K. and Sekar, V., 2012, December. New opportunities for load balancing in network-wide intrusion detection systems. In Proceedings of the 8th international conference on Emerging networking experiments and technologies (pp. 361-372).

[27] Tripathy, S.S., Mishra, K., Roy, D.S., Yadav, K., Alferaidi, A., Viriyasitavat, W., Sharmila, J., Dhiman, G. and Barik, R.K., 2023. State-of-the-art load balancing algorithms for mist-fog-cloud assisted paradigm: A review and future directions. Archives of Computational Methods in Engineering, pp.1-36.

[28] Imperva. Sticky Session. https://www.imperva.com/learn/availability/sticky-session-persistence-and-cookies/.(Accessed 10 December 2023).

[29] Lectron, 2023. Least Connection Load Balancing, (July). https://www.lectron.com/docs/fivem/load-balancing-algorithms/least-connection-load-balancing/. (Accessed 10 December 2023).

[30] Oracle, 2023. Load Balancer Policies,(March). https://docs.oracle.com/en/us/iaas/Content/Balance/Reference/lbpolicies.htm\Policies/IPHas.(Accessed 10 December 2023).

[31] IBM. Learn how load balancing optimizes website and application performance.https://www.ibm.com/topics/load-balancing. (Accessed 10 December 2023).

[32] Microsoft Azure Learn. Use Source Network Address Translation (SNAT) for outbound connections.https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections.(Accessed 10 December 2023).