Cloud Computing & Information Security Implementation Of Firewall

Realized by:
Douha BOURACHED & Oumaima BENLAMHAIRA
Supervised by: Pr. RAFALIA Najat
Ibn Tofail University, Faculty of Science, Departement of Computer Science
Master Big Data & Cloud Computing
2022-2023

Abstract

Cloud computing has become increasingly popular among businesses and organizations due to its cost-effectiveness and scalability. However, with the rise in cloud adoption comes an increase in security risks. As more organizations move their data and applications to the cloud, security becomes a critical concern. One of the most effective ways to ensure security in the cloud is by using a firewall to control access to the internet. In this article, we explore the benefits of firewall access control in the cloud, and how it can be used to protect against threats such as unauthorized access, malware, and data breaches. We also discuss the key features to look for when selecting a cloud-based firewall, including scalability, ease of use, and integration with other security solutions. Finally, we present our use case where we successfully implemented a cloud-based firewall to enhance the security posture and reduce the risk of cyberattacks that might reach the virtual machine we had deployed on Azure cloud. By implementing firewall access control in the cloud, organizations can ensure that their data and applications are secure, and their business operations remain uninterrupted.

Keywords: *Cloud Computing, Security Risks, Firewall, Cyberattacks, Virtual Machine.*

I. Introduction:

Information security is one of the most important concerns for companies using cloud computing. With the rapid growth of cloud technology, companies are storing more and more sensitive data on remote servers, which can expose them to numerous security risks. Threats can come from internal or external sources and include online attacks, configuration errors, data leakage and privacy breach. The importance of information security in cloud computing is further emphasized by the fact that companies are increasingly relying on the cloud for critical activities, such as supply chain management, financial transactions and internal communications. A disruption in information security can have serious consequences for a company's reputation and customer trust.

Therefore, it is critical that companies take steps to protect sensitive data in the cloud. Companies must assess information security risks, adopt effective security strategies, and ensure that cloud providers take steps to protect data. This can include the use of encryption technologies, access controls and authentication, identity and access management techniques, and compliance with cloud security regulations and standards. By ensuring information security, organizations can realize the many benefits of cloud computing while minimizing the risks to their business.

II. Problematic Statement:

One of the main security problems on the cloud is the risk of unauthorized access. Cloud providers typically use a shared security model where the provider is responsible for securing the infrastructure while the customer is responsible for securing their own data and applications. This can lead to security gaps if the customer doesn't implement the proper security measures. Another security issue is data breaches. Cloud providers are targeted by cybercriminals because they store a large amount of sensitive data. If a cloud provider's security is compromised, it can result in a massive data breach that affects multiple customers. Finally, cloud providers can also be vulnerable to distributed denial of service (DDoS) attacks that can disrupt services and cause damage.

III. Objective:

The objective of this project was to improve the security of the cloud infrastructure of companies and prevent unauthorized access to sensitive data by implementing a firewall solution.

Implementing a firewall solution on the cloud can bring significant advantages to businesses and organizations. Cloud-based firewalls offer enhanced security by protecting resources from unauthorized access and malicious attacks, reducing the risk of data breaches. They are also cost-effective compared to traditional on-premise solutions as they do not require physical hardware or ongoing maintenance costs.

Cloud-based firewalls are scalable, allowing businesses to add resources as needed without worrying about hardware limitations. Centralized management is another key benefit of cloud-based firewalls, as they can be managed from a single console. Compliance is also a consideration for many industries, and cloud-based firewalls can help meet regulatory requirements by providing robust security features and maintaining audit trails for resources. Overall, implementing a firewall solution on the cloud provides businesses with a secure and cost-effective way to protect their resources from potential security threats.

IV. Background:

a. The Impact of Cloud Services on Security:

Cloud computing services offer a wide range of benefits, including cost savings, scalability, and flexibility. However, each type of cloud service presents unique security challenges that must be addressed to ensure the security of data and applications in the cloud.

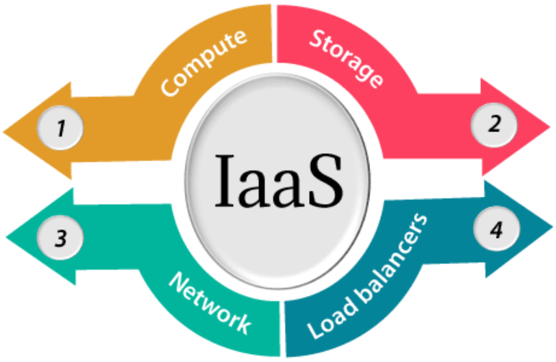


Figure 1: Infrastructure-as-a-Service

Infrastructure-as-a-Service (IaaS) is a cloud service model that provides virtualized computing resources, such as servers, storage, and networking, over the internet. While IaaS provides organizations with more control over their cloud infrastructure, it also requires organizations to take on more responsibility for securing the infrastructure. In an IaaS environment, organizations must implement their own security measures, including firewalls, to protect their virtual machines and data.

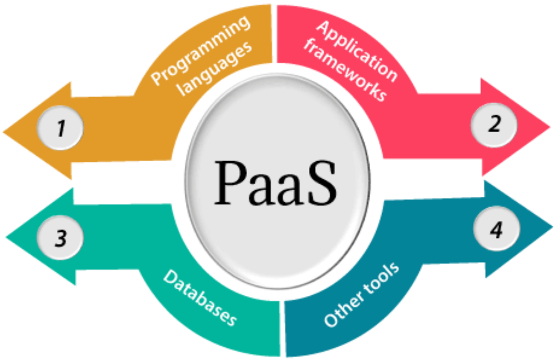


Figure 2:Platform-as-a-Service

Platform-as-a-Service (PaaS) is a cloud service model that provides a platform for developing, running, and managing applications in the cloud. PaaS services typically include pre-configured components for application development, such as databases, middleware, and programming languages. While PaaS providers typically provide some security features, such as access control and authentication, organizations are still responsible for securing their applications and data in the PaaS environment.

Business Services
1
Document Management
2
SaaS
3
Social Networks
4
Mail Services

Figure 3:Software-as-a-Service

Software-as-a-Service (SaaS) is a cloud service model that provides software applications over the internet. SaaS providers are responsible for securing the software and infrastructure used to deliver the service, but organizations are responsible for securing their own data and user access to the service.

The use of multiple cloud services and platforms can create security challenges, as it can be difficult to implement consistent security measures across an organization's entire cloud infrastructure. In addition, the lack of physical control over cloud infrastructure and data can create vulnerabilities that can be exploited by malicious actors.

To address these security challenges, organizations must implement effective security measures, such as firewalls, to protect their cloud infrastructure and data. A firewall in a cloud environment can help to prevent unauthorized access to sensitive data and applications, as well as block malicious traffic and attacks.

b. Cloud-Related Security Challenges:

- **Lack of Visibility and Control:**

One of the main advantages of using cloud-based technologies is that the client does not have to manage the resources (such as servers) necessary for operation. However, delegating responsibility for the daily maintenance of software, platform, or IT assets can result in a decrease in visibility and control over these assets.

This can hinder the organization when attempting to:

- Test the effectiveness of our security controls since there is no visibility on the tools and data of the cloud platform
- Implement incident response plans since there is not necessarily full control over cloud resources
- Analyze information about your data, services, and users which is often crucial for identifying incorrect usage patterns associated with a security breach.

- **User Access Control:**

User access control, which is almost always the responsibility of the user, is a critical challenge for cloud security, regardless of the type of cloud service used. However, as with on-premises security solutions, user access control in the cloud can be difficult, especially if the cloud service does not have very robust control settings.

- **Data Privacy Issues:**

If a cloud service lacks cybersecurity, sending sensitive data can make it vulnerable to theft. Even when strong cybersecurity measures are in place, transferring data to the cloud can violate confidentiality agreements between a company and its customers. This can result in fines, trade restrictions, and damage to reputation

c. Meaning of Cloud Security:

Among the security measures, we have:

- **User Access Control:**

Internet access control can play an important role in an organization's data security. It can limit access to certain websites and restrict the use of certain protocols and applications that could pose a security risk. Here are some examples of the positive impacts of internet access control on data security:

<u>Protection against malware:</u>

Malicious websites can contain viruses, spyware, and other malware that can infect users' computers and compromise data security. Internet access control can help to block access to these sites and reduce the risk of infection.

<u>Prevention of data leaks:</u>

Internet access control can help to limit the use of certain protocols and applications that could be used to transfer sensitive data outside of the organization's network. For example, employees can be prevented from using cloud storage services or instant messaging services that are not approved by the organization.

<u>Reduction of phishing risks:</u>

Internet access control can help to block access to phishing websites, which are designed to deceive users into providing sensitive information such as usernames and passwords. By limiting access to these sites, the risk of data theft through phishing can be reduced.

- **Data encryption in the cloud:**

Data encryption in the cloud refers to the use of cryptographic techniques to protect data stored in the cloud. Cloud computing services are becoming increasingly popular for storing data due to their relatively low cost, accessibility, and scalability. However, data security in the cloud is a major concern for many organizations, especially when it comes to sensitive or confidential data.

Data encryption in the cloud can be achieved in several ways, including:

End-to-end encryption:

Data is encrypted before being sent to the cloud and is only decrypted when the user connects to the cloud to retrieve the data. This method provides a high level of security as the data is encrypted throughout its transit and storage in the cloud.

Server-side encryption:

Data is encrypted once it reaches the cloud server and is stored in encrypted form. This method is less secure than end-to-end encryption as the data is decrypted once it reaches the server, leaving a window of opportunity for attackers.

Database encryption:

Data is stored in an encrypted database hosted in the cloud. This method provides a high level of security as the data is encrypted even when stored in the database.

- **Firewall:**

Connecting personal computers to other computer systems or to the internet offers many advantages, such as ease of collaboration with other people, resource sharing, and increased creativity. However, this can be at the expense of complete network and device protection. Hacking, identity theft, malware, and online fraud are common threats that users may face when exposing their computers to a network or the internet. Proactive protection is essential when using any type of network. Users can protect their network from the worst dangers by using a firewall.

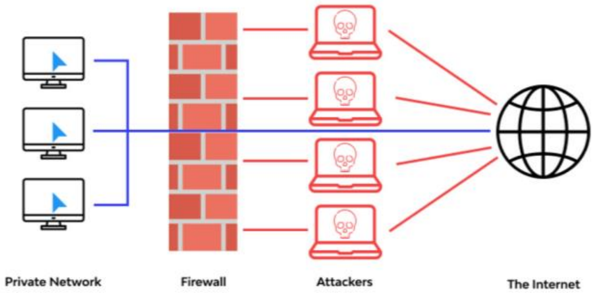
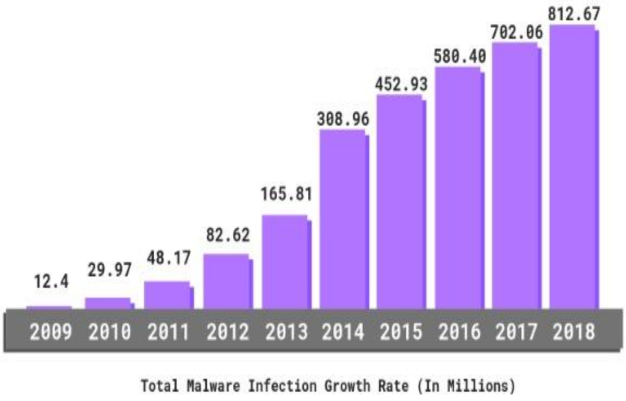
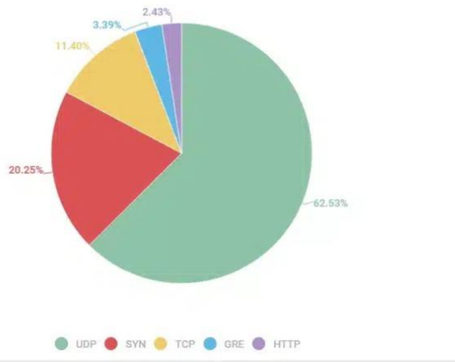


Figure 4:Cloud Firewall

A firewall is a key component of cloud security. The firewall is a security system that allows monitoring and control of incoming and outgoing network traffic of a computer system. In the context of cloud computing, the firewall is an essential element of security to protect the user's data and resources in the cloud. The firewall in the cloud can be configured to block unauthorized traffic and filter malicious data from the internet. It can also be configured to restrict access to cloud resources from specific IP addresses or to allow access only from certain IP address ranges. Firewalls in the cloud are also capable of detecting and blocking distributed denial-of-service (DDoS) attacks. Next-generation firewalls use advanced threat detection technologies to identify and block sophisticated attacks, such as phishing attacks and SQL injection attacks.

Here are some statistic of malware infection growth rate and DDos attacks by types over 2022:





Distribution of DDoS attacks by type, Q2 2022 (download) kaspersky

There are several studies that have shown that implementing access controls on internet traffic can help reduce the risk of DDoS attacks and phishing attacks. Here are some statistics that you may find helpful:

A study by the Ponemon Institute found that 56% of organizations that suffered a data breach did not have effective access controls in place.

According to a report by Radware, organizations that implemented web application firewalls (WAFs) to control access to their web servers experienced a 99.99% reduction in DDoS attack volume.

The Verizon 2021 Data Breach Investigations Report found that phishing attacks accounted for 36% of all data breaches. Implementing access controls, such as multi-factor authentication and limiting access to sensitive information based on job roles, can help prevent phishing attacks.

A study by Imperva found that organizations that implemented access controls and other security measures saw a 73% reduction in DDoS attack volume compared to those that did not.

Overall, these statistics suggest that implementing access controls on internet traffic can be an effective way to reduce the risk of DDoS attacks and phishing attacks. However, it's important to note that no security measure is foolproof, and organizations should also implement other security measures, such as regular software updates, employee training, and vulnerability scanning, to further reduce their risk of cyber-attacks.

V. Use Case:

In our case we have worked on a specific case of access control which is controlling access to the internet in the cloud using a firewall. Controlling access to the internet refers to the act of monitoring and regulating the use of the internet within a particular network or system. This can involve implementing restrictions or permissions for certain users, devices, or applications to ensure secure and appropriate usage of the internet. Controlling access to the internet can significantly enhance security by mitigating a range of cyber threats. By monitoring and regulating access to the internet, organizations can prevent users from accessing potentially harmful websites or downloading malicious software, reducing the risk of cyber-attacks such as phishing, malware infections, and ransomware.

Access controls can also prevent unauthorized access to sensitive information and data. By implementing role-based access controls and limiting access to certain applications and systems, organizations can ensure that only authorized personnel can access critical data, reducing the risk of data breaches and cyber-attacks. Furthermore, access controls can enable organizations to monitor and audit user activity, enabling them to detect and respond to potential security breaches quickly.

In addition to these technical controls, access controls can also promote a culture of security awareness and responsibility within organizations. By establishing clear policies and guidelines around internet access, organizations can educate employees about the importance of safe browsing practices and encourage them to report any suspicious activity. This can help to reduce the risk of insider threats and ensure that all employees are aligned with the organization's security objectives.

Overall, controlling access to the internet is a critical component of any comprehensive cybersecurity strategy. By implementing effective access controls, organizations can reduce the risk of cyber threats, protect sensitive information, and promote a culture of security awareness and responsibility.

The Step-by-Step Guide to Implementing Our Solution

The steps we followed to carry out our project are as follows:

The first step is to create a resource group. In Azure, a resource group is a logical container for grouping together related Azure resources such as virtual machines, storage accounts, and virtual networks. A resource group helps you manage and organize your resources, as well as simplifies the process of deploying, updating, and deleting those resources. It is a way to manage all the resources related to a specific project, application, or environment. By organizing resources into a single resource group, you can apply a consistent set of policies, permissions, and tags to all the resources in that group. Additionally, you can easily view and manage the status, performance, and cost of all the resources in a resource group using the Azure portal, PowerShell, or the Azure CLI.

The second most important component in the virtual network in Azure is a virtual network. A virtual network is a logical representation of a network in the cloud. It is a private network that you can create and configure within the Azure infrastructure, and it enables you to securely connect Azure resources to each other, to on-premises networks, and to the internet.

A virtual network provides isolation and segmentation of network traffic between resources within the network. You can define subnets (in our case, three subnets) within the virtual network, each with its own IP address range, and then deploy resources such as virtual machines, Azure App Services, and other services into those subnets (in our case, it was a virtual machine). You can also configure virtual network security by creating network security groups to filter inbound and outbound traffic to and from resources in the network.

Then comes ***the third step***, which is the deployment of a virtual machine (VM) which is an emulation of a computer system. It behaves like a physical computer but runs on shared hardware, providing a more cost-effective and scalable way to run your applications. Azure virtual machines allow you to choose from a wide range of pre-configured virtual machine images or create your own custom images. You can also select the size of the VM, the operating system, and the disk size, depending on your specific needs. Azure virtual machines can be used for a variety of purposes, such as running applications, hosting websites, running virtual desktops, and running databases. They can also be used for testing and development, as well as for disaster recovery and backup purposes. The virtual machine deployment process is as follows:

1. Select the subscription, resource group, and region where we want to deploy the VM.
2. Choose an operating system image for our VM. We could select from pre-configured images or use our own custom image.
3. Choose a VM size that meets our needs in terms of CPU, memory, and storage.
4. Provide a unique name for our VM, a username, and a strong password.
5. Configure the network settings for our VM, including the virtual network, subnet, and IP address.
6. Choose whether we want to enable or disable the public IP address for our VM.

The fourth step is the firewall deployment:

1. Configure the firewall: Once the firewall VM is deployed, we needed to configure the firewall rules to allow inbound and outbound traffic as per the requirements. This includes configuring network security groups, firewall policies, and access control rules.
2. Integrate the firewall with the virtual network: After the firewall is configured, we had to integrate it with the virtual network. This involves creating a network interface for the firewall VM and attaching it to the virtual network and subnet. (Note that the private IP address will be used when we create the default route)

The fifth step is the creation of a route table. In Azure, a route table is a collection of rules or routes that specify how network traffic should be directed in a virtual network. A route table contains a list of routes, each of which specifies the destination address range and the next hop type (such as a virtual appliance, virtual network gateway, or internet) for that destination. When a network packet arrives at a virtual network interface, the virtual machine's operating system consults the associated route table to determine how to forward the packet.

And last, we have the application rules and network rules:

1. An application rule is a type of firewall rule that allows you to define fine-grained control over network traffic based on the application layer protocol or URL. With application rules, you can create rules that allow or block traffic based on the specific application or URL being accessed, regardless of the underlying IP address or port number.

Application rules are commonly used to allow or block traffic for specific applications or websites within a virtual network, and they are often used in conjunction with network security groups to provide additional security for virtual machines and services.

2. Network rules are a type of firewall rule that allows you to control network traffic based on the source or destination IP address, port number, or protocol. With network rules, you can create rules that allow or block traffic to and from specific IP addresses or ports, providing a way to secure your virtual network and its resources.

Network rules are commonly used to control traffic within a virtual network, and they are often used in conjunction with network security groups to provide additional security for virtual machines and services.

Now that those rules were set, we can control the machines allowed to access our virtual machine via IP addresses and the websites a user is allowed to access or not, and therefore ensure a powerful security system to protect our virtual machine.

VI. Discussion:

In this study, we implemented a firewall on a virtual machine to enhance security in cloud computing. The firewall successfully controlled access to and from the virtual machine, providing an additional layer of security. However, cloud computing presents various security risks that organizations must mitigate through a comprehensive security strategy, including regular security assessments and audits. Overall, the implementation of a firewall is an effective security measure, but ongoing monitoring and improvement are essential for securing cloud computing environments.

VII. Conclusion:

The firewall successfully controlled access to and from the virtual machine, demonstrating the importance of implementing security measures to protect cloud environments.

Our findings highlight the need for organizations to take a proactive approach to cloud security. Implementing firewalls, as we did in this study, is just one of the many security measures that organizations can take. Organizations must also conduct regular security assessments, monitor their cloud environments, and implement additional security measures as necessary to address new and emerging threats.

In conclusion, while cloud computing offers many benefits, security risks cannot be ignored. Implementing security measures like firewalls is crucial for protecting cloud environments, but it is only one part of a broader security strategy. By taking a comprehensive approach to security, organizations can mitigate the risks associated with cloud computing and ensure the safety of their data.

VIII. References:

Jonatha Anselmi, Danilo Ardagna, Mauro Passacantando.” Generalized Nash equilibria for SaaS/PaaS
Clouds”, European Journal of Operational Research 236 (2014) 326–339
Thomas. (2020, February 10). Différence Entre IaaS, SAAS et paas. WayToLearnX.from https://waytolearnx.com/2019/03/difference-entre-iaas-saas-et-paas.html
“IaaS, paas, Saas : Quelles sont les différences ?,” Red Hat - We make open source technologies for the enterprise. [Online].
Kessler, T. (2017). Sécurité de l’information avec le cloud computing. Bulletin des médecins suisses, 98(45), 1493-1494.
KESSLER, Thomas. Sécurité de l’information avec le cloud computing. Bulletin des médecins suisses, 2017, vol. 98, no 45, p. 1493-1494.
Kessler, Thomas. "Sécurité de l’information avec le cloud computing." Bulletin des médecins suisses 98.45 (2017): 1493-1494.
M. rediriger directement vers: “Qu'est-ce que le cloud computing ?,” ServiceNow. [Online]. Available:
https://www.servicenow.com/fr/products/it-operations-management/what-is-cloud-computing.html.
“Les Défis de Sécurité dans le cloud computing: Problèmes et solutions ...” [Online]. Available:https://www.researchgate.net/publication/260733580_Les_defis_de_securite_dans_le_Cloud_Computing_Problemes_et_solutions_de_la_securite_en_Cloud_Computing.
Futura, “DÉFINITION: Cloud computing - informatique EN NUAGE: Futura Tech,” Futura, 08-Apr-2015.
[Online]. Available: https://www.futura-sciences.com/tech/definitions/informatique-cloud-computing-11573/.
Elmrabti, A. A., Abou El Kalam, A., & Ouahman, A. A. (2012, April). Les défis de sécurité dans le Cloud
Computing: Problèmes et solutions de la sécurité en Cloud Computing. In 2012 National Days of Network Security and Systems (pp. 80-85). IEEE.
ELMRABTI, Almokhtar Ait, ABOU EL KALAM, Anas, et OUAHMAN, Abdellah Ait. Les défis de sécurité
dans le Cloud Computing: Problèmes et solutions de la sécurité en Cloud Computing. In : 2012 National Days of Network Security and Systems. IEEE, 2012. p. 80-85