PROJECT TITLE
FIREWALL SIMULATION

PROJECT REPORT

Submitted in the partial fulfilment of the requirements

for award of the

Six Months Online Certificate Course

in

Cyber Security

Course Duration: [22-01-2024 to 21-07-2024]

By

Name:Mallepaka Saikiran
(Ht.No. 2406CYS113)

Under the Esteemed Guidance

Prof. B.SateeshKumar

DIRECTORATE OF INNOVATIVE LEARNING & TEACHING (DILT)

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

(Formerly SCDE_SCHOOL OF CONTINUING AND DISTANCE EDUCATION)

Kukatpally, Hyderabad, Telangana State, INDIA- 500 085

JULY 2024

TABLE OF CONTENTS

1. Abstract

Today, almost every business uses the internet for better communication, from individuals and partners, which raises many concerns about the safety of the network or computer connected to Internet. Internet security has become a major problem with existing devices. It also seems that stopping bad things will not affect us all. So, this study explores how to use a firewall to protect the internet by exploring different technologies and types of firewalls, as well as how it can help protect the internet. The settings set for the firewall and how to turn it off will also be discussed. It is suggested that the use of firewalls has played an important rolein preventing widespread security threats on the internet, which should provide a solution to the problem and make it more efficient, safer internet. However, from this study, I suggest that the safety of the internet should be improved so that the security and access of Internet users is not compromised by neglecting or compromising themselves. perdition or fear.This information is about rumours about the use and configuration of a web application firewall that protects the purpose of the application by supporting incoming requests and their restrictions by the program. These principles, in turn, are mastered by users of traffic through the application. Because many web applications, including those operated by the government, are generally easy to use, it is important to quickly introduce new procedures to prevent unauthorized access to data. Learn Apps WebWall offers flexible, customizable and easy-to- submit application solutions. However, there are concerns about processing data used to learnsystems that may in some cases correctly violate firewall rules. These concerns were raised by commentators.

2. Introduction

In order to ensure the security of filling and sending relevant information to customers for continued use on today's sites, organizations need to go through various controls, and this leads to increased risk research. However, there are some challenges that people have to face in this era. First, one of the main problems of using surface vehicles is the need to identify them and determine which vehicles should be blocked. low delay response for related applications. Another difficult problem of using them is the poor quality, or how much the tool determines that the user is always bad and can interfere with their work, which can make the use of the tools more difficult than they want.

The first reason we use well-known technology to create web applications. Many web development sites, such as PHP and ASP, are aware of security vulnerabilities, and opponents use these vulnerabilities to implement applications. The same is ultimately true for database engines that use this application.

The second reason is also the width of the attack. The main users of the web application connect to the Internet. Anyone can try to kill or attack your app from the online beast.

Almost all of these attacks fall into several categories, including SQL injection, web crawling, remote data sharing, lack of HTTP headers, robots, crawlers, and scanners. Search for weak web applications on the Internet, crash of large web applications and more.All of these attacks can be prevented. One way is to save code levels, which is hardly the job of the developer. In addition, it requires repair, maintenance, and repair across multiple stages of theapplication. An easy option is to purchase a Web Application Firewalls (WAF) and install them in front of the Web server to prevent multiple attacks. This provides central protection for web applications against excessive usage and inefficiency.

Microsoft Azure also offers WAF services that provide protection against site overuse and crashes. Azure Application Firewall is a feature of Azure Application Gateway (Process Load Equalizer 7) and is primarily designed to protect Web applications from attacks such as SQL injection, cross-site scripting, and many more. It also implements the Open Web Application Security Project (OWASP) Statute Series. The Azure WAF service allows you to select some or all of the rights from the OWASP set of statutes.Azure Application Gateway has an IP address or public prefix, and application users will use that IP address to connect to the application gateway. The application controls a transit gateway and usually the transition to the appropriate end of the set. You can list application services, virtual machines, virtual machines, or even any other IP address in the set shown in the implementation part.

According to a recent survey, 72% of research companies have been hacked in the last 24 months. Most attacks occur well on the application layer (layer 7 of the OSI standard) - as this is still the most vulnerable area. While low-level devices are ultimately insecure, over theyears, network systems have become so complex that they are difficult to crack and have some drawbacks. In addition, operating systems, web servers, and encryption engines are alsosecure - as they are usually provided by several vendors, all of which have large enough usersto identify them early and fix them quickly. However, the applications on the site are different - usually different (although they replace different rules - such as some functions) and are usually managed by a consumer or a consumer. On the other hand, this reduces the average security of the rules (because information is scarce for companies operating in different industries), and conversely, the disadvantages are rarely seen before they are used. This is why the disadvantages of web applications are still 1:10 higher than those of a browser / operating system.

In recent times, the changing nature of site usage has started to increase a lot, with each passing bad and bad applications and bad attempts and more and more for this to happen sometimes. The development of web applications as well as the appearance of the Internethas changed a lot. Most companies and individuals started using website apps in a day. The Website is an important link for all users around the world, where personal information aboutWebsite users is stored in an archive. Some activities contain sensitive information about users, such as e-banking. Information on business security, passwords, and financial permissions. User data security is a major concern for all e-commerce owners and administrators, as it has had a profound impact on website usage throughout its history. Manyattackers can hack some web applications and access personal information around the world by exploiting vulnerabilities in some web applications. Such cyber threats can cause financialdamage to many parties as well as private companies and other construction companies. Various network security has been developed to identify and prevent various network threats.The idea of identifying a malicious website and sending information to another website where the same attacker can attack or use the same attack method plays an important role. The process needs to evolve faster and faster, and the system works with many web walls to identify, alert, prevent and track an attacker.

3.Literature Review

Many sites have vulnerabilities that are very easy to use. According to research conducted by the Web Application Security Consortium, "More than 13% of all research sites may be at risk. Approximately 49% of web applications are faulty. High risk (urgent and critical) For automated testing, however, the reports and evaluations come from the white box in detail, and the rules for identifying vulnerabilities, which can reach 80-96%, are well developed. most recent in many areas in these areasbut also the hearts that the government dislikes. Routledge believes that "the application to the gold standard of information security, the DataManagement Security Guide, offers the simple combination of information, expertise, ideas, and tools that IT professionals need today. Now in its sixth edition, this 3,200-page, 4- volume-independent file is under development.in the CISSP dialog and is updated annually. Each annual update, most recently in Volume 6, introduces changes to CBK in accordance with new policies and technologies.

In 2011, Larry L. Peterson and Bruce S. Davie published the fifth issue of their book Computer Networks, which explores all aspects of computer networks. Danny Yee writes in his review: “In many ways, computer networks: a process to be seen in a larger communication guide sentences used to describe problems in its use). Connectivity problems (ethernet and signal rings, coding, framing, and error detection); for packet switching and routing; bridges, Internet access, IP and IPv6, DNS and multicast; end-to-end protocols (UDP, TCP, RPC, and conflict processing); and endpoints between endpoints (bulk terrestrial instruction, encryption, compression).

One way is to follow the hotspot analysis with reliable applications and data and provide data from these sources reliably, to say that only reliable data can be part of the application. semantic queries such as keywords and SQL generators. He developed an idea to analyse the SQL injection. It monitors SQL authentication using MD5 renaming and algorithm. Use codefor grammatical sentences to check the SQL injection in the URLs. There is no change in the application code according to their method. Resistance has been investigated and reduced. The increase in the number of registered users allows site applications to apply without delay and protect the application from SQL injection. It describes the process of preventing DDoS attacks against REST Web services, in which the source is identified by specific URLs created by the HTTP process. REST web servers easily use DDoS. It tracks the movement of the IP address using highly requested URLs and time scale as custom.There are many ways for a web application to crash. However, many different factors make up the most. Some of them are described below. These are the attacks that can be prevented (for the sake of difference) with the dynamic measurement methods described in this article. However, it is important to keep in mind that the list according to the SANS Top 25CWE list includes all the weakest points. An in-depth explanation goes back to other categories. Especially SQL Injection, are attack vectors that try to execute code on a target machine. In its simplest form, it is risky if the rate entered by the user returns a very high query and sends it to the translation target. The disadvantage of this attack often stems from insufficient access, which does not clean up or destroy the importance of measurement. Access to Parameter is a generalconcept for changing constraints sent by a server on demand, usually to set parameters thatthe server does not need. The purpose of this operation is to make the application requesting the application work as usual, it can be performed as needed. Modifications are examples of malfunctions, but the attack can also focus on application / server (DoS) failures or identity theft.

The complexity and number of rules required to create a WAF is important for its adoption. Therefore, look for the natural right path and try to establish the rule of thumb. That is, supporting the WAF and the right to education.One of the main benefits of WAF training is the ability to store applications without installation or addition. Companies that use commercial or non-commercial products often have WAF-specific standards that protect theirapplication, but companies that make special or well-designed applications. The site needs to take care of it. In such a situation, WAF training would be the best solution - providing personal protection without the need for a lot of work. The best place for a WAF is a traffic restriction or no and / or a residential area is part of a residential area. The following companies must decide on these solutions: - Portals and other dynamic, flexible websites - Banks and companies accept and accept tests against cyber threats. - Government agencies - not least almost all of them use special websites / special rules that do not employ security experts to protect them (do not know the reputation of the military).Web Pages: By considering the current link URL and the number of URLs listed on the page, you can determine how the current user's behavior follows the code. If the reference to the original URL is not found or is scarce, it may appear that the user is behaving badly, which means he is doing something wrong. Such a request can be ignored, preventing the application from affecting the hard-browsing environment. Plot size: If you have three matched sizes for each user metric specified on the page, you can subtract whether the current size fits the “normal” size. This is a common server function, which can be explained quickly afterwards. By controlling and accepting irrelevant needs, the application can prevent any attack, including SQL injection and scripting. Of course, the effectiveness of this method depends on the magnitude of the statistical behavior, which in turn depends on the number of structural data and the percentage of stress. bad or wrong efforts involving all situations.

4.Problem statement

In addition to the only engineering problems associated with creating an HTTP runtime, there are significant issues with creating and implementing WAF self-paced applications. These relate to the cost of the stored data, the stored data, and the application data considered in measuring the data set.

Scope of data- One of the key factors influencing WAF’s ability to deal effectively with negative results is its ability to use reference data to evaluate it. If there is too much information and the WAF does not accept the legal benefits that are not yet included in the information used, there is too much and the WAF needs to be pre-trained, which can greatly affect performance (similar to that found in neural networks). Data retention time (DRT), which is the analysis of data, depends on the design of such users. changed weekly. It is unlikely that there is a reliable model that could help measure DRT, and this would be well known to administrators. It is important to note that the shorter the DRT, the more suitable the WAF is to modify the application, but there is a risk of a counterfeit server attack.

Context of Parameter- From a user’s point of view, a web application (or part of its business) is a machine whose behavior and status depend on the user’s behavior. This means that in some cases the importance of lots or numbers or usage depends on the current situation. A similar example is money transfer, where the user can access the account number as a valuable item, but the user does it without login. As with Scope data, the best content will depend on the needs of the specified application, and in many landings, it is used as content, option and URL referring to and / or the conversation ID as a display.

Storage of data-WAF sets the message that the user sends to the destination site. This means that you will also receive personal information, including authorization information (login name and password). However, if the WAF is able to measure the results relative to past data, it will retain the data over time. This leads to a significant problem retrieving resources and servers with sensitive data. Because the WAF does not know in advance that the data is understandable, it must apply the same rules to all metrics. One solution is to use the key to hide the stored data (preferably from the external onruntime of the WAF). The other is to store all the data in RAM only. The first solution is to invest a lot of money and always count on the energy required for encryption and decryption. The last way to put the backup file to a restore point is to leave the window open until a new file is written. A good but bad solutionis to define a parameter that contains soft data.

In terms of data collection and analysis, two different operating systems can be discussed. One is the learning experience (TL) and the other is the continuous learning scenario (CL). The TL situation requires the WAF president to clearly open and exit the course. In this mode, the system writes the parameter values based on the value used or puts them in a general value design or collection. At the end of the course, WAF switched to "working" mode, where it did not set a standard, only comparing approval costs with the experience learned. There are several reasons for this situation: - The size of the data stored at that time does not need to be taken into account. The data that are considered for standardized assessment are the data that are collected in the course. - Not all historical data need to be protected. At the end of the study period, all data can be sample or reasonable results. This also eliminates the problems of storing sensitive data mentioned earlier. - WAF defence attacks focus on your training.

5. Objectives

The first step in setting up a home firewall. Due to the difficulties and strength of the hosted site, the usual process / legacy and application required to open the site will not be realized due to the difficulties and strength of the day. to grow up in today's world. Therefore, it is important to understand what these goals are, where the WAF will fit into the security solution, and thus provide security to these aspects.

In addition to financial constraints, decide to replace the firewall cloud WAF, hardware, or software as a firewall requirement.

Another important decision in this process is whether to develop or further develop the WAF in order to achieve better solutions. In both cases, the following procedure is performed.

The security code for firewalls for web applications
The black / bad name tag allows traffic to scan and prevent / prevent any malicious requests. WAF should be involved in ongoing practice, otherwise it will play a small role.

Allows active lists / templates for which all apps / traffic is blocked. This leads to poor performance, so constant and continuous changes will be the key to making the model work well.

This type of hybrid security combines advantages and disadvantages, minimizes accidents, and improves web security. So here we see the need for hybrid security models to be able to compare well with negative models. This challenge alleviates the problem, leading to better security of web applications.

Choosing the right type is very important and the user should keep in mind the details of their needs.

The WAF type indicates the initial start-up type, in addition to the quality of the web application the hybrid storage type should be the starting point for any web business. Once this is done, it is important to know how to maintain the right value from the WAF

Create and manage WAF forecasts

To create or integrate any site service, developers must adhere to certain firewall application rules. So, when I create a firewall, I plan to set the values according to the appropriate rules. This course covers the research process, vehicle inspection, and OWASP for the popular music MO.

Following the amendment of the law, the legal administration must be linked to changes in individual legal provisions. I plan to implement individual plans by adapting them to my situation and needs identified during planning. For example, I would not work for a community and a region. I will see that the WAF policy is constantly updated so that the business process does not change.

I will ensure that the safety information and assessments that the WAF receives from security experts are used to determine eligibility when applying to the WAF. It also allows the security user to monitor and manage storage. I think you need to be there to check for undetectable machine errors. Most importantly, I will ensure that WAF policies provide protection for existing applications.

Be smart WAF with AI and ML

By constantly reviewing the WAF policy update against the risks involved, I was able to complete the security screening process of my application and improve my understanding of the attacks that occur on my site to make firewall web applications more create best. I am constantly learning from previous attack history and international threat documents and being made aware of the security risks of my existing applications, which allows for greater risk reduction.

Firewall and its approach

We’ve used firewalls and other training, and in fact, the issue isn’t off the internet. We have indoor firewalls that divide the parking lot from one building or another to another, for example. The fire wall is used to prevent the fire and the fire is spread slowly until the fire department extinguishes it. The same is true for car fires, which divide passengers in the engine compartment. In their last book on Internet firewalls, Cheswick and Bellovin stated that the Internet firewall has the following characteristics: a key in two or more networks through which all vehicles will pass (solid tents); The device can be operated and admitted to all vehicles. In the show, Bellovin later said, "Firewalls are a problem between 'us' and 'them' because of the lack of trust of 'them'." The first power network appeared in the late 1980s and was used by sailors to split networks into small LANs. Avolio, F. and Ranum. In these terms and using the words Cheswick, W. and Bellovin, "we" can mean "us". And "they" can be English departments. Such firewalls are shown to prevent problems caused by a single LAN affecting all networks. This was done so that the English department could install applications on its own network and manage its network as required by the department. Stations are kept under the router so that problems with network management errors or noise applications do not interfere with the entire school network.

Expand and repair the safety wall below. These firewalls are made from something called bastion support. Probably the first fire station of its kind to use filters and proxies for Digital Equipment Corporation and integrated with the DEC firewall. Brian Reid and an engineering team at DEC's Network Systems Lab in Palo Alto began developing the DEC firewall. The first commercial firewall was installed and began on June 13, 1991 for the first customer, the East Coast pharmaceutical company, Avolio, F., and Ranum. Over the next few months, Marcus Ranum of Digital developed security proxies and modified other firewall codes. The electronic device is designed and called DEC SEAL (Secure Output Link). DEC SEAL has an external system called gate gatekeeper, an internet system that can communicate, gateway and location on Mailhub.

Firewall technology can be used to secure a network from a system unit to a single storage port that will keep the Intranet connected to the public internet, thereby paving the way for complete cyber security. This can be further used to isolate the sub-network for providing cyber security within this related organization. The firewall usually uses three functions to protect the network:

1. Filter package
2. Circuit proxy
3. Proxy application

Packet filter

Packet filtering scans the same header as the IP address monitored by the access control, without any changes. Because the work is simple, speed and efficiency always follow this procedure. There is one better! The work does not require special supervision from users and is completely independent, but that does not mean that they do not understand it properly. Understanding depends on the key.

Packets can be filtered as follows: IP address (location and address), TCP / UDP port. Firewalls of this type can block connections to and from guests on multiple networks. This cost is small because they use router software and complete security due to their system configuration and complexity.

Circuit proxy

Proxy managers are the ones who have to look at all the messages in their package and this is an important difference between proxy networks and package wall filters. Assuming the location is given. Circuit, assuming confirmation of arrival, takes his (her) address and destination address.

Compared to filter filters, gateway applications use more processing data and add more security as well as more rules and regulations. It is usually used by one or more owners and includes custom software developed for this organization. The gateway application provides alist of services that control access to global services such as Telnet and FTP. An external usercannot use the service unknowingly. Many companies use email. The gateway can function as a user reception and reception for remote users.

Proxy application

Depending on the filter wall of the packet and the peripheral proxy, the proxy of the application is more complex. The application proxy first understands the data in the application and then tries to correct users and assess the level of data risk. However, this complex but comprehensive feature comes at a price; it is usually necessary to reconfigure the user with a loss of clarity.

An important difference with many network firewalls is that they handle traffic directly through them, which means you must have a blocked IP address or Internet address to use them. Network layer firewalls are usually very fast and can be used almost transparently. Application-level firewalls are defined, operated by proxy servers, do not allow direct network operation, and perform complex logging and monitoring of traffic through them. Because applications are software running only on a firewall, they are a good place to perform access and control in a variety of ways.

Limitations of firewall

All the best in the world has its limits. Limitations make everything fall apart. It shows us what to use and what to avoid. C. Mahalakshmi described some of the limitations of firewalls, not only reducing its need, but also working hard to understand the limit. Listed below are some firewall restrictions for you to know.

a) Firewall security is restricted in the area and it is impossible to fight the enemies inside it.
b) Firewalls are not the best way to prevent some malicious activities and viruses (like trojans)
c) Configuring package filters is not user friendly and difficult, so the resulting error is the result does not work. It is a complex system in which mistakes can be made easily, resulting in openness and security

6. Methodology

Design processes are designed to provide all product users with the best precautions and protection with the highest safety precautions. The main idea is to identify the purpose of the joint operation and send the data to the command-and-control center, which sends the data to another coordinator, to rule together with the same opponent and the same opponent. the type of strike as a general unit. Thus, basically, the body takes responsibility when the homeowner sees the attack and sends the necessary information to start sending the information to another customer and take the necessary measures to prevent such incidents in the first place. In addition, the system has safety precautions that prevent the point of failure throughout the body, such as other central and control areas in the event of a collision or stop, or any function in the main control area, does not operate in reverse. Management and administration of the institution above and below. Check the user interface to make sure the system is not changing and make sure the system is running smoothly. The main purpose is toreveal conflicting information to other users through a new type of site wall modification that can send and receive threat information and track received information.In this section, I have discussed the points to consider when creating a firewall application. In addition, there are a number of ways and means to implement a firewall in the system that I have focused on. In the main project, I will focus on developing firewall applications with knowledge of the following concepts and topics.

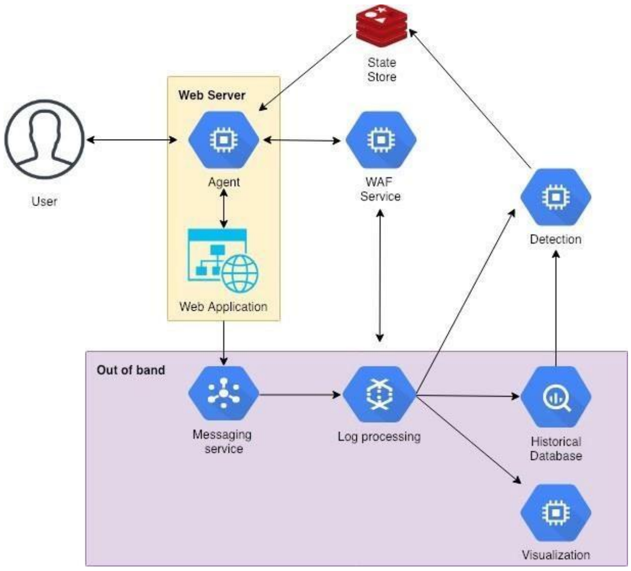


Figure 1: web application firewall

The system will take immediate action when it detects an attack and triggers a threat, and alerts other firewalls after reporting the attack information with command and control to counter the threat. The first step to starting the system is to identify the attacker and then sendthe results to the Office and Control, which forwards the information to all users. Connect to be aware of early action against the threat, depending on the type of firewall. and the rules involved, the centralized Web Firewall system is just one upgrade that can be applied to all Web Firewall technologies, giving it a unique new way to make the Web Firewall service different from Web Firewall to install. locating and managing process capabilities. The joint venture users updated the new threat detection information and took steps in the existing attack data, based on the information they received; the type, date, and time of the attack, and the IP address of the attacker. The figure below shows the process:

Agent

If you use proxy mode for WAF, the software is configured on a web server modelled according to the hardware configuration. While this facilitates server connectivity, it can affect storage space more effectively and provide fewer web servers with less distributed capacity.

Cloud

By using cloud providers as a WAF solution, web servers can take advantage of easy setup and unlimited visibility of capabilities. This is accomplished by allowing a third party to be inthe middle of traffic between web servers and users. The disadvantages of this plan are the increased latency due to traffic passing through the cloud provider (which can be reduced if it is the only provider for the web application) and the fate of third-party information.

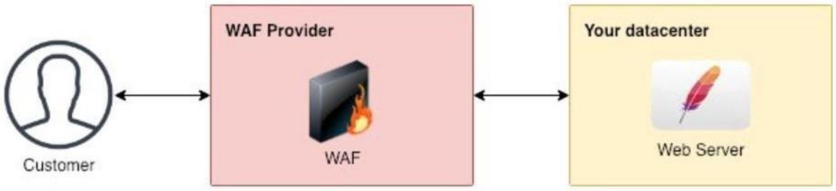


Figure 2: WAF cloud mechanism

Network location

As defined for external or graphical devices, depending on the size of the organization, the concept of network implementation can be difficult when using WAF solutions. In an environment with multiple libraries that store applications that need to be maintained, complete WAF coverage (whether planned or scheduled vehicle copies) is established. can be a dangerous job. This can lead to significant investments in network transmission that require unused resources or switching to WAF solutions.

False positive rate

One of the biggest problems with WAF blockchain solutions is the lack of quality that they create. Negative prices can indicate how many users are blocked when they do not strike, which can lead to financial loss and damage to reputation. One of the main reasons that WAF solutions do not enter blockchain mode is that false positives sufficiently affect users, and the security of the team is bound to fail. Do not block the attack and just turn the medication into a scene that cannot stop it.

Extensive

Because the WAF needs to monitor traffic and determine whether or not to block it, the delay is exacerbated by the WAF application. Depending on the location and performance of your network, you may be limited to applications that rely on low-level responses to operate or engage their customers.

Prevents attacks from web applications

To benefit from this model, we need to be able to determine which ones are best protected. This reduces the regular delays for users and eliminates the possibility of adverse effects on them. To achieve this, we need to decide which one to put in "inline" mode:

Traffic management

Vehicle management is one way to determine if the vehicle equipment is operating in internal mode, where all requests are reviewed and blocked by the WAF when counted, i.e., the web application. This allows applications that have patience for delays to monitor their traffic and increase delays only when a threat is detected and requests are blocked.

Fingerprint management

By recognizing the traffic in the operating system, you can track the fingers that cause the site to request attacks and easily pass them through the WAF (increased latency). These fingers can be removed by linking to the requested location (IP address, user ID, user, or links) or by some fingerprint to be removed. can be added manually (e.g., 0-finger date or known stroke style). Once the operating system receives this fingerprint and adds it to the General Purchasing section so that the agent knows that it needs to run the WAF operation, this can bestarted by an intermediary. decided to send special fingers. by the WAF.

Netblock Management

Another option for traffic control is network block monitoring. This means that some known ISPs, utility providers, or other utilities have an increased risk of being attacked by them (either as an open source or anonymous source, such as a TOR) can be customized by the WAF function. This is done by switching the state store to a network of IP addresses of service providers or network members to let the agent know that he or she needs to send the message to the WAF.

False rate control

In order to find a way to prevent users who do not make the website requesting an attack, we must first distinguish between the weaknesses of the inspection system (DFP) and the weaknesses of the investigation. standard block (BFP). When we accept that there are flaws in the investigation process (meaning that the idea that a request will be the source of the complaint when it is not) we will focus on the absence. malfunctions and blocking processes (their request are suspended and prevented the normal user from accessing the software on the web server). One important thing to consider is that while it may remove the negative elements, the various applications will make it the wrong one that they do not have. Willingness to accept in the face of the risk of resistance to completion. Due to the fact that the false positives can be reduced by closing another frame around demand, the lower the negative value we need another frame we need, and this also means that more time from the attack has been tested. using the web application. Any application must address its own type of threat against user interference in order to find the true value of false information. This chapter will focus on how to prevent a user's request from being blocked and how we can best use the information we provide before deciding which one should be sent to a web server.

Statistical Data Significance

The following decisions apply only to the CL case, as all material in the TL case can be considered valid and valid. However, data collected by CL WAF may be inaccurate or even malicious - because these are written by anonymous, often anonymous individuals. For WAF to work properly, the following assumptions should be followed: The value of the inaccuracy measure is only a small fraction of the total results identified. The reason for this requirement is clear: a significant amount of error data instructs WAF to accept them as valid input. What is not clear is how to set the level "uncritically" for specific files. There is currently no specialist research on the distribution and grouping / distribution of key metrics for on-site services, so there is no clear information. The level of this priority is usually determined by the system administrator based on their previous experience, changing needs, and knowledge of the application. However, a critical measure has several characteristics that can be used to optimize the distribution. According to the writers' experience, many unnecessary numbers can be divided into the following groups: - Numerical numbers. Most creative people are numbers. In addition, key numbers are used to manage the status of the application, to check the archive, and so on. - Select values. These are usually tied to user preferences. Therefore, only a small number of values can be seen. Both of these groups are easily identified by simple heuristic methods. Therefore, it is necessary to add algorithms to estimate parameter values in engineering, although there are still limitations that do not fall into this category. (e.g. names) and is also a common target for attempted theft.

7.algorithms

1. Signature-Based Detection

1. Description: Utilizes predefined patterns or signatures to detect known threats such as SQL injections, cross-site scripting (XSS), and other common attack vectors.
2. Pros: Effective against known threats; low false positive rate.
3. Cons: Ineffective against zero-day attacks and new threats; requires regular updates.

2. Anomaly-Based Detection

4. Description: Establishes a baseline of normal traffic behavior and detects deviations from this norm, which may indicate an attack.
5. Pros: Capable of detecting new and unknown threats; adaptive to evolving attack patterns.
6. Cons: High false positive rate if the baseline is not accurately defined; requires continuous learning and adjustment.

3. Behavioral Analysis

7. Description: Analyzes the behavior of users and applications over time to identify patterns that may indicate malicious activity.
8. Pros: Can detect sophisticated attacks that follow unusual patterns; reduces false positives by considering behavior over time.
9. Cons: Requires extensive data collection and analysis; can be resource-intensive.

4. Heuristic Analysis

10. Description: Uses a set of heuristic rules or criteria to evaluate and identify potentially malicious activity.

11. Pros: More flexible than signature-based detection; can identify new and emerging threats.

12. Cons: Can generate false positives if heuristic rules are too broad; requires fine-tuning.

5. Rate Limiting

13. Description: Limits the number of requests a user or IP address can make in a given timeframe to prevent Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

14. Pros: Effective against volumetric attacks; easy to implement.

15. Cons: Can impact legitimate users if not configured properly; not effective against low-and-slow attacks.

6. IP Reputation Filtering

16. Description: Blocks or restricts traffic from known malicious IP addresses based on reputation databases.

17. Pros: Effective against known bad actors; reduces the attack surface.

18. Cons: Requires up-to-date reputation data; can block legitimate traffic if IP addresses are incorrectly flagged.

7. Geolocation Filtering

19. Description: Blocks or restricts traffic based on the geographical location of the request.

20. Pros: Useful for targeting attacks from specific regions; easy to configure.

21. Cons: Can block legitimate users from certain regions; not effective against attackers using proxies or VPNs.

8. Content Filtering

22. Description: Inspects the content of HTTP requests and responses to detect malicious payloads.

23. Pros: Effective against content-based attacks like SQL injection and XSS; can inspect both request and response payloads.

24. Cons: Can be resource-intensive; requires regular updates to detection rules.

9. Tokenization and Encryption

25. Description: Protects sensitive data by replacing it with tokens or encrypting it during transmission.

26. Pros: Prevents data breaches by securing sensitive information; enhances compliance with data protection regulations.

27. Cons: Can introduce latency; requires robust key management practices.

10. Machine Learning

28. Description: Employs machine learning algorithms to analyze traffic patterns and detect anomalies indicative of attacks.

29. Pros: Adapts to new and evolving threats; improves detection accuracy over time.

30. Cons: Requires substantial data for training; can be complex to implement and manage.

11. Automated Threat Intelligence

31. Description: Integrates with threat intelligence feeds to receive real-time updates on emerging threats and automatically adjusts detection rules.

32. Pros: Keeps the WAF up-to-date with the latest threats; reduces manual effort in updating rules.

33. Cons: Dependence on the quality and timeliness of threat intelligence feeds.

12. Contextual Awareness

34. Description: Considers the context of requests, including user behavior, session history, and application state, to enhance detection accuracy.

35. Pros: Reduces false positives by understanding the broader context; improves detection of complex attacks.

36. Cons: Requires comprehensive data collection and analysis; can be resource-intensive.

37.By combining these algorithms and techniques, WAFs provide robust protection against a wide range of cyber threats, helping to secure web applications from both known and emerging attack vectors.

8.Implementation

Azure Application Gateway the Azure Web Application Firewall (WAF) provides protection against intrusion into a Web site through a variety of uses and vulnerabilities. Web applications are targeted by malicious attacks, which usually use unknown techniques. Scripting between SQL injection and sites is one of the most common challenges.All of the WAF lists below are in the WAF Code. You may create multiple policies and associate them with Application Gateway, client, or custom policies according to the terms of use of the gateway. This way, you can have separate rules for each field after the Application Gateway, if necessary. For more information on WAF policies, see Creating WAF Policies.

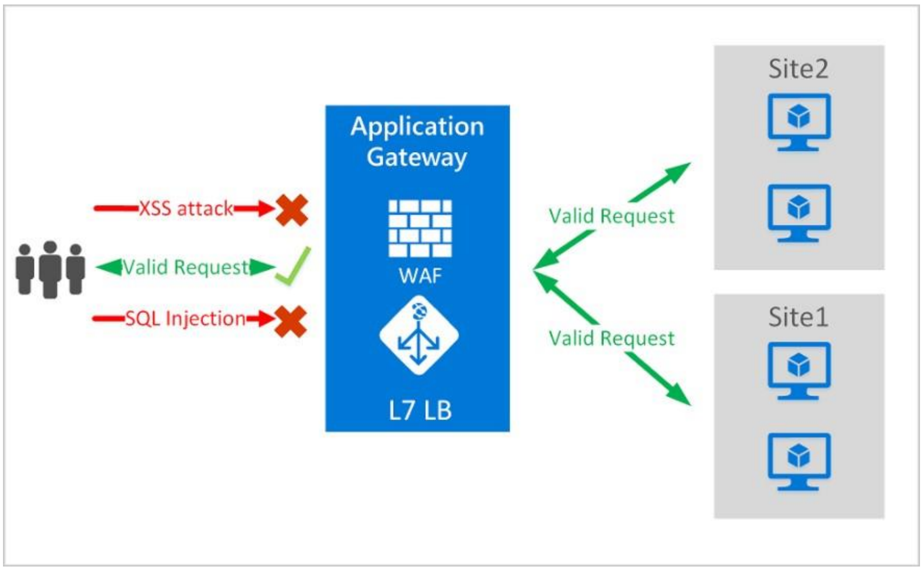


Figure 3: Application Gateway

The Application Gateway complies with the Application Delivery (ADC) standard. Includes Secure Sockets Layer (SSL), formerly known as Transport Layer Security (TLS), decommissioning, sharing all cookies, the sharing environment, content routing, the ability to host multiple sites, and improved security.

Improving Application Portal security includes TLS policy administration and full TLS support. Application security has been strengthened by integrating WAF into the Application Gateway. The combination of web applications avoids the disadvantages. And it provides a central location that is easy to set up and maintain.

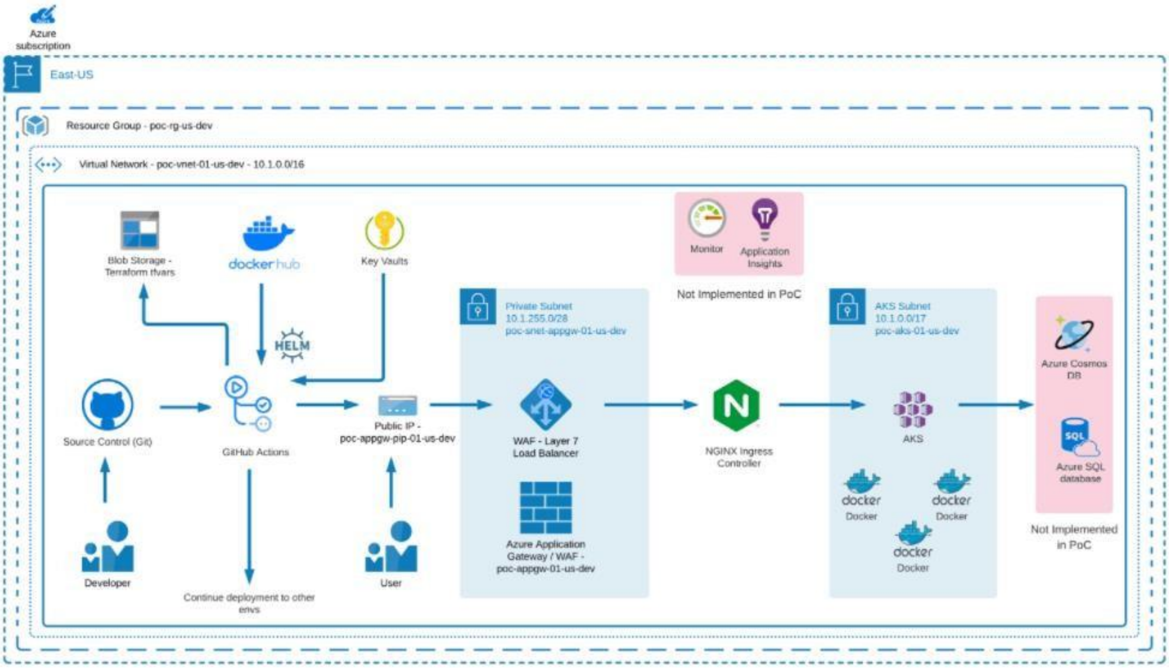

Azure subscription
East-US
Resource Group - poc-rg-us-dev
Virtual Network - poc-vnet-01-us-dev - 10.1.0.0/16
Blob Storage - Terraform tfvars
docker hub
Key Vaults
HELM
Source Control (Git)
GitHub Actions
Public IP - poc-appgw-pip-01-us-dev
Developer
Continue deployment to other envs
User
Private Subnet 10.1.255.0/28 poc-snet-appgw-01-us-dev
WAF - Layer 7 Load Balancer
Azure Application Gateway / WAF - poc-appgw-01-us-dev
Monitor
Application Insights
Not Implemented in PoC
NGINX Ingress Controller
AKS Subnet 10.1.0.0/17 poc-aks-01-us-dev
AKS
docker Docker
docker Docker
docker Docker
Azure Cosmos DB
Azure SQL database
Not Implemented in PoC

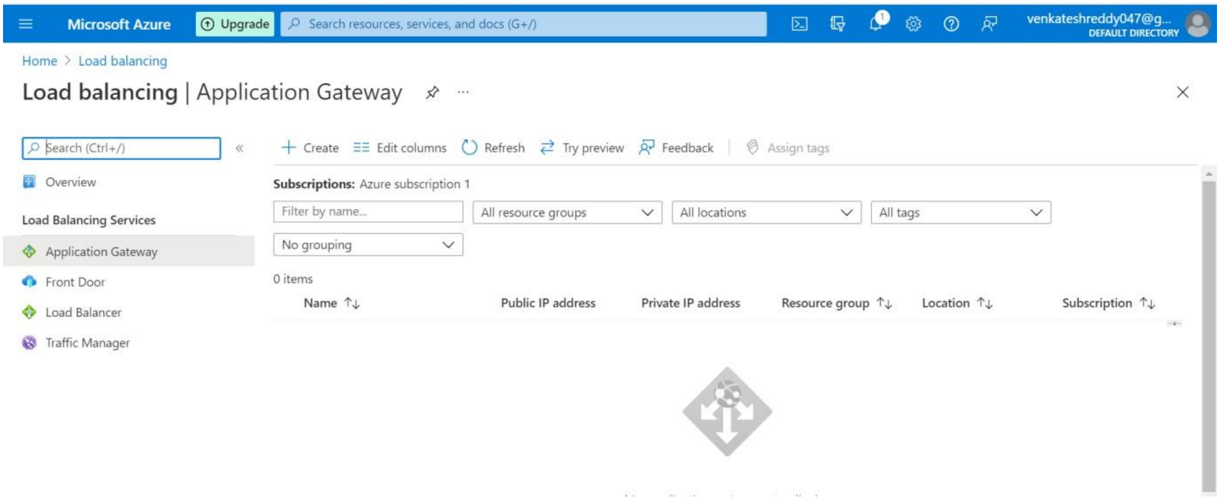
Figure 4:WAF services

There are two types of web application firewall:

- Search Status: Use this method to diagnose, understand and learn about network connections, which includes identifying vulnerabilities. Monitor and set all alarms. Make sure diagnostics is selected on the WAF engine and turn it on. Note that WAF does not block incoming requests while in search mode.
- Type of protection: prevents access to official attacks. The attacker received a "Unauthorized Access 403" stop and the link was lost. Security mode records these attacks on the WAF machine.

Azure configuration

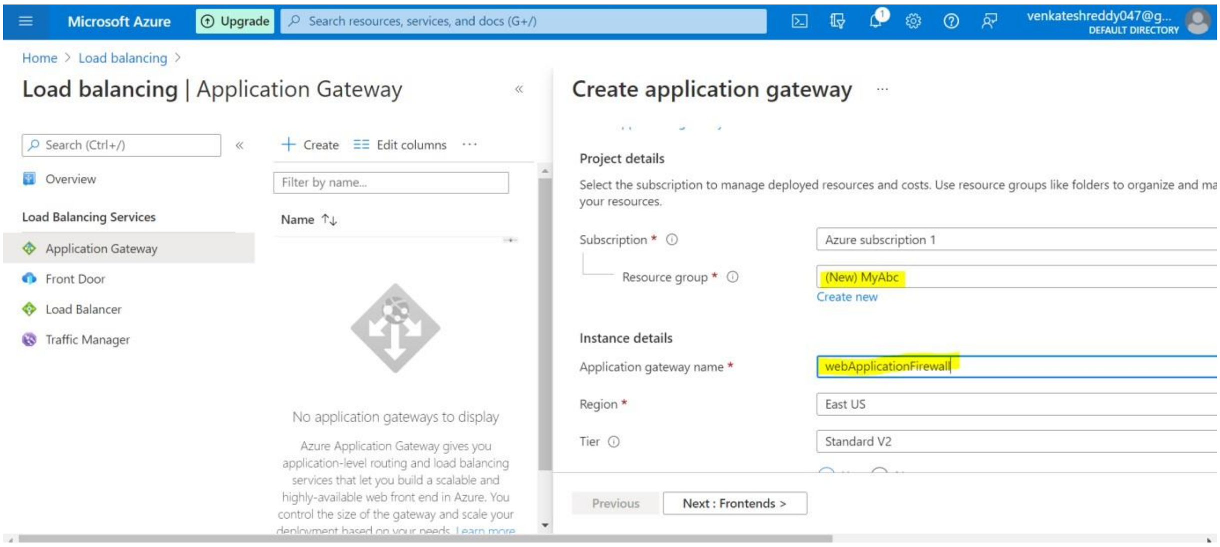
- Enter the Azure Portal, enter the Azure Market, and find your way
- Select the Application
- Click Create



Subscriptions: Azure subscription 1

0 items

- If you selected WAF V2, select Yes or No for Auto Scaling
- If you selected Yes in the Support Automatic Scaling section, enter the Minimum and Maximum Scale units.



No application gateways to display

Azure Application Gateway gives you application-level routing and load balancing services that let you build a scalable and highly-available web front end in Azure. You control the size of the gateway and scale your deployment based on your needs. Learn more

Create application gateway

Project details

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

Subscription *: Azure subscription 1

Resource group *: (New) MyAbc

Instance details

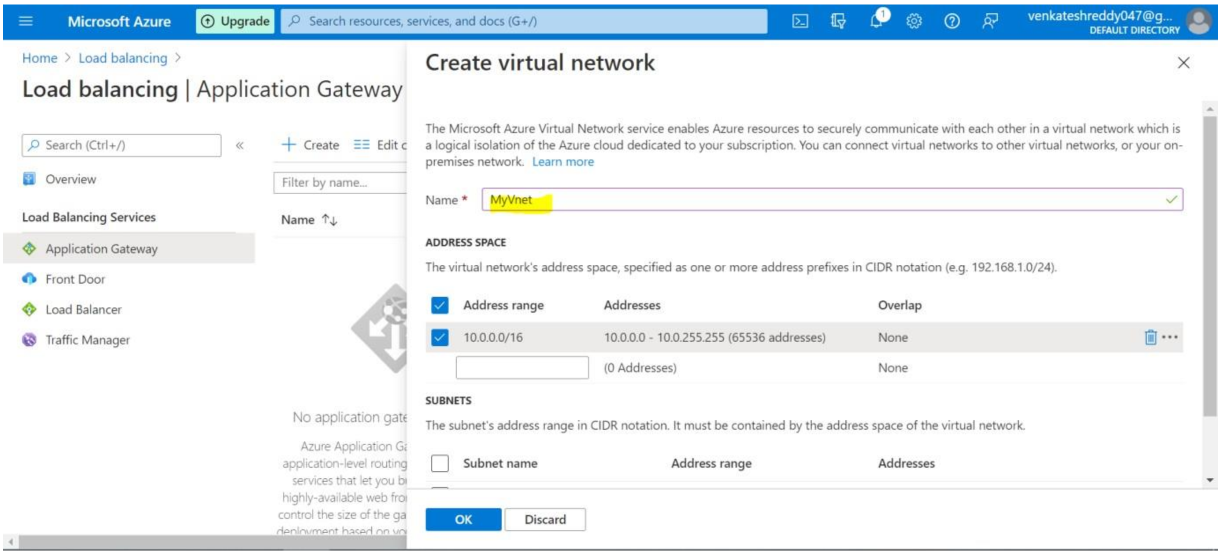
Application gateway name *: webApplicationFirewall

Region *: East US

Tier: Standard V2

- If you selected No in the Enable Automatic Scaling section, go to Units

- Firewall Management "Enabled"
- Set the firewall mode to "Father" or "Long" according to your taste
- Keep the existing space as a unit
- Keeping HTTP2 "Disabled"
- In the Configure Virtual Network section, select an existing virtual network or create a new one by selecting Create New.



Create virtual network

The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with each other in a virtual network which is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or your on-premises network. Learn more

Name * MyVnet ✓

ADDRESS SPACE

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

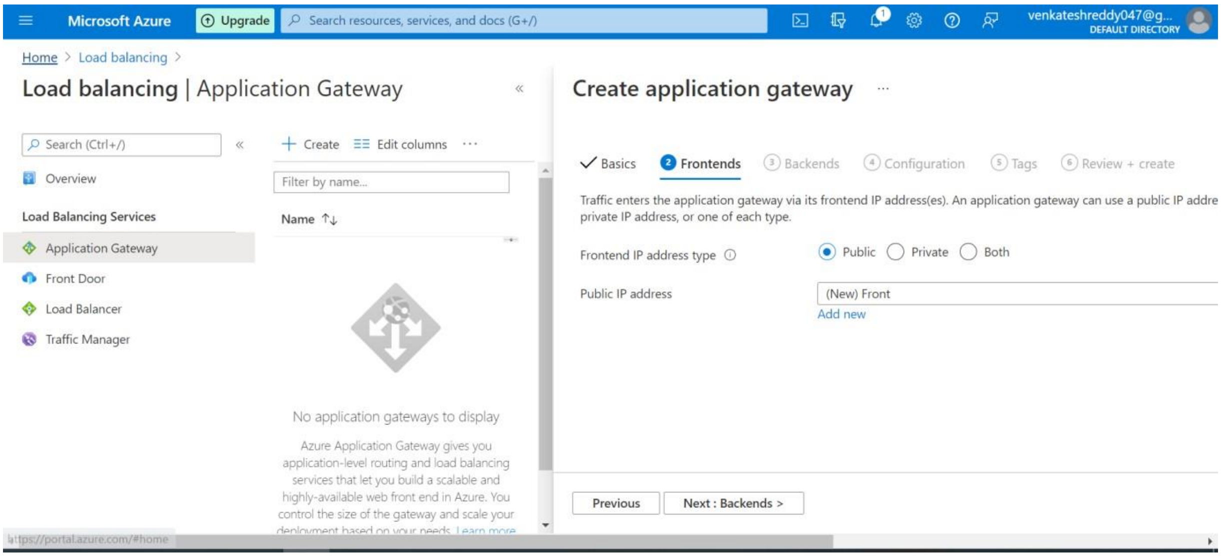
☑ Address range	Addresses	Overlap
☑ 10.0.0.0/16	10.0.0.0 - 10.0.255.255 (65536 addresses)	None
	(0 Addresses)	None

SUBNETS

The subnet's address range in CIDR notation. It must be contained by the address space of the virtual network.

□ Subnet name	Address range	Addresses

OK Discard


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
venkateshreddy047@g...
DEFAULT DIRECTORY
Home > Load balancing >
Load balancing | Application Gateway
Search (Ctrl+/)
Overview
Load Balancing Services
Application Gateway
Front Door
Load Balancer
Traffic Manager
+ Create
Edit columns
Filter by name...
Name ↑↓
No application gateways to display
Azure Application Gateway gives you application-level routing and load balancing services that let you build a scalable and highly-available web front end in Azure. You control the size of the gateway and scale your deployment based on your needs. Learn more
https://portal.azure.com/#home

Create application gateway

✓ Basics ② Frontends ③ Backends ④ Configuration ⑤ Tags ⑥ Review + create

Traffic enters the application gateway via its frontend IP address(es). An application gateway can use a public IP addre private IP address, or one of each type.

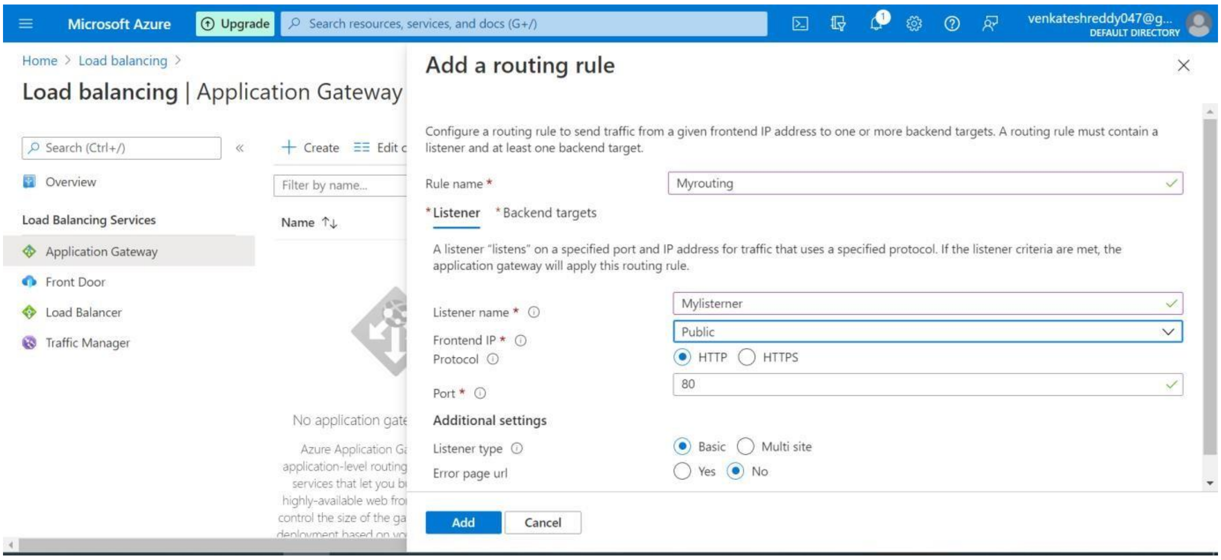
Frontend IP address type ● Public ○ Private ○ Both

Public IP address (New) Front

Add new

Previous Next : Backends >

- Write a name for the background
- Keep the background Add to "No" without target
- Choose the right goal and purpose, there are many options, choose the one that suits your needs



Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | venkateshreddy047@g... DEFAULT DIRECTORY

Home > Load balancing >

Load balancing | Application Gateway

Add a routing rule

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name * Myrouting

*Listener | *Backend targets

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener name * Mylisterner

Frontend IP * Public

Protocol ● HTTP ○ HTTPS

Port * 80

Additional settings

Listener type ● Basic ○ Multi site

Error page url ○ Yes ● No

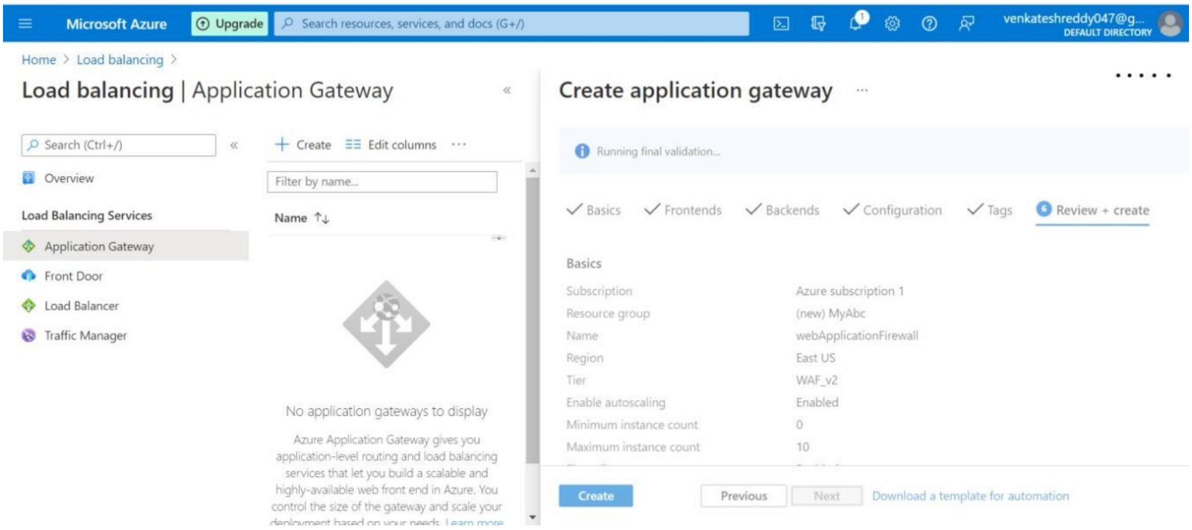
Add | Cancel

The routing rule also requires a destination date. Click the "Recovery Options" tab

Select the object selected as "Backend Pool"

Select the after-sales plan required by this policy. In our example, the postdoctoral pool we designed at Level 4 above can be selected

To configure HTTP, click the "Add New" button to create a new HTTP site. An HTTP Web site defines the behavior of this policy, including port and protocol protocols for Web sites and Web sites such as cookie-based social networking and networking.



Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | venkateshreddy047@g... DEFAULT DIRECTORY

Home > Load balancing >

Load balancing | Application Gateway

Create application gateway

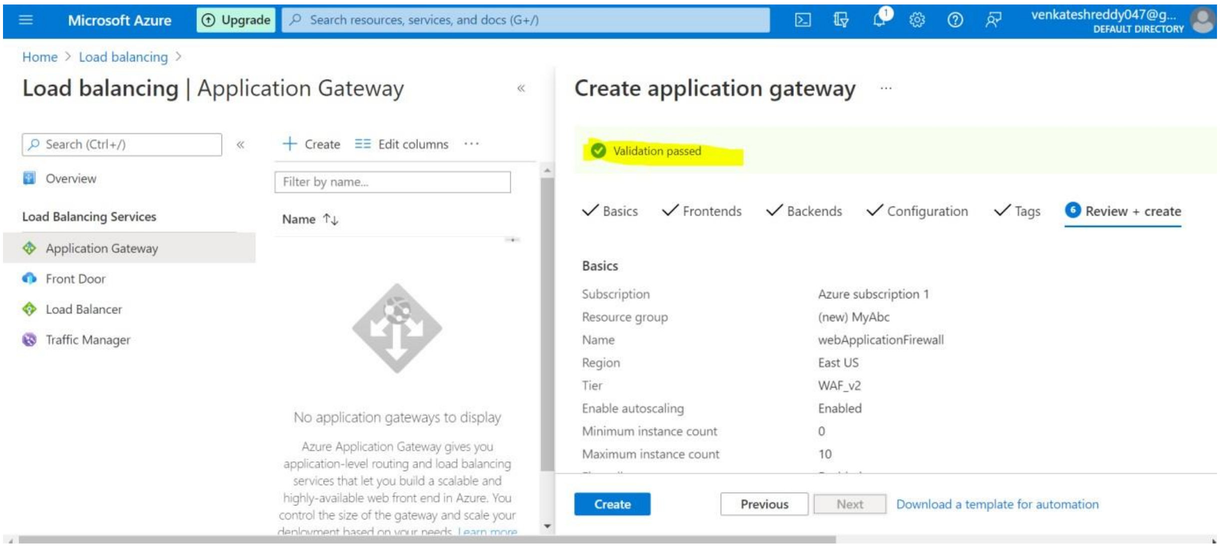
Running final validation...

✓ Basics ✓ Frontends ✓ Backends ✓ Configuration ✓ Tags | Review + create

Basics

Subscription	Azure subscription 1
Resource group	(new) MyAbc
Name	webApplicationFirewall
Region	East US
Tier	WAF_v2
Enable autoscaling	Enabled
Minimum instance count	0
Maximum instance count	10

Create | Previous | Next | Download a template for automation



Load balancing | Application Gateway

No application gateways to display

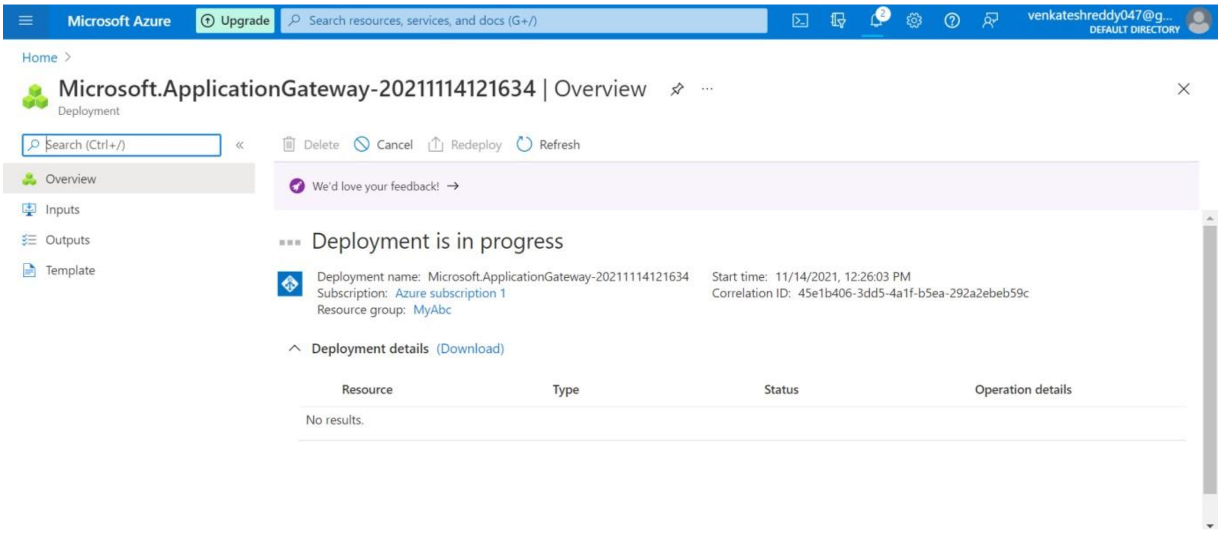
Azure Application Gateway gives you application-level routing and load balancing services that let you build a scalable and highly-available web front end in Azure. You control the size of the gateway and scale your deployment based on your needs. Learn more

Create application gateway

Validation passed

Basics

Subscription	Azure subscription 1
Resource group	(new) MyAbc
Name	webApplicationFirewall
Region	East US
Tier	WAF_v2
Enable autoscaling	Enabled
Minimum instance count	0
Maximum instance count	10



Microsoft.ApplicationGateway-20211114121634 | Overview

Deployment

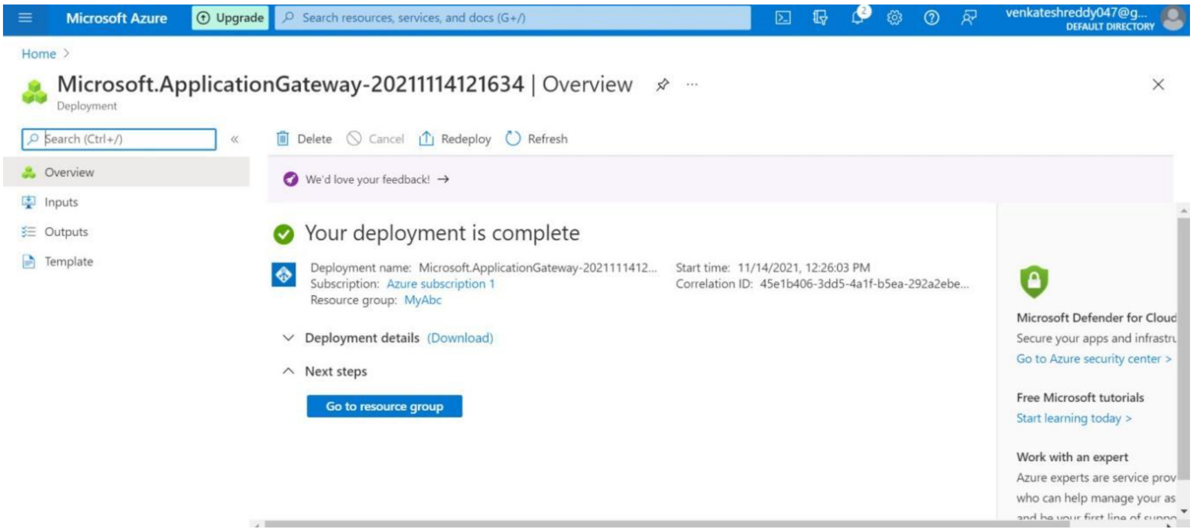
Deployment is in progress

Deployment name: Microsoft.ApplicationGateway-20211114121634
Subscription: Azure subscription 1
Resource group: MyAbc

Start time: 11/14/2021, 12:26:03 PM
Correlation ID: 45e1b406-3dd5-4a1f-b5ea-292a2ebeb59c

Deployment details (Download)

Resource	Type	Status	Operation details
No results.			



Microsoft.ApplicationGateway-20211114121634 | Overview

Deployment

Your deployment is complete

Deployment name: Microsoft.ApplicationGateway-2021111412...
Subscription: Azure subscription 1
Resource group: MyAbc

Start time: 11/14/2021, 12:26:03 PM
Correlation ID: 45e1b406-3dd5-4a1f-b5ea-292a2ebe...

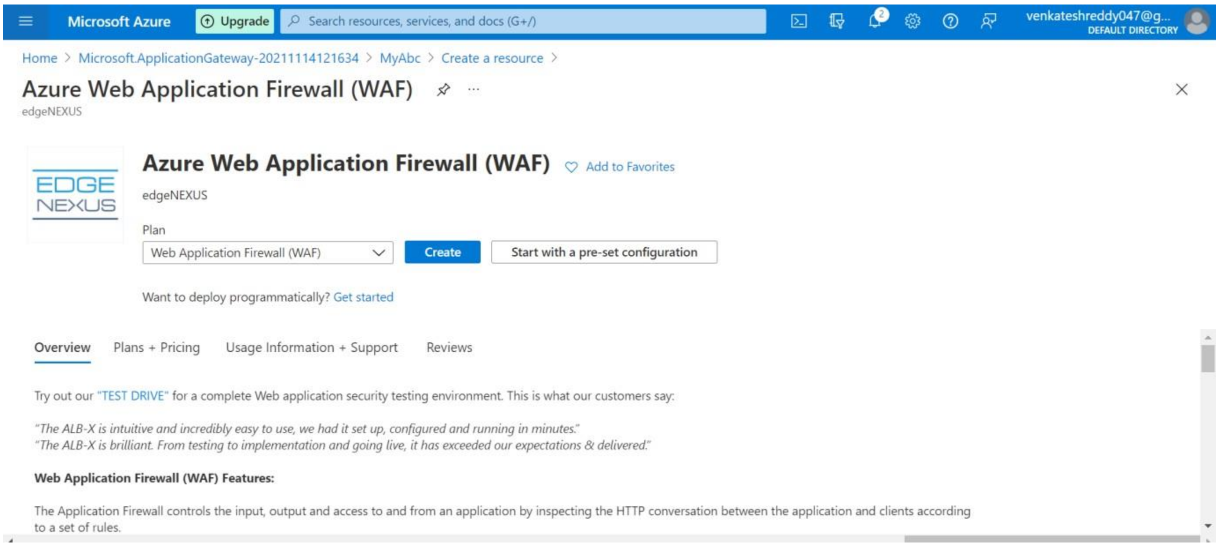
Deployment details (Download)

Next steps

Microsoft Defender for Cloud
Secure your apps and infrastru
Go to Azure security center >

Free Microsoft tutorials
Start learning today >

Work with an expert
Azure experts are service prov
who can help manage your as


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
venkateshreddy047@g...
DEFAULT DIRECTORY
Home > Microsoft.ApplicationGateway-20211114121634 > MyAbc > Create a resource >
EDGE NEXUS
Add to Favorites
Create
Start with a pre-set configuration
Overview
Plans + Pricing
Usage Information + Support
Reviews

Azure Web Application Firewall (WAF)

edgeNEXUS

Azure Web Application Firewall (WAF)

edgeNEXUS

Plan: Web Application Firewall (WAF)

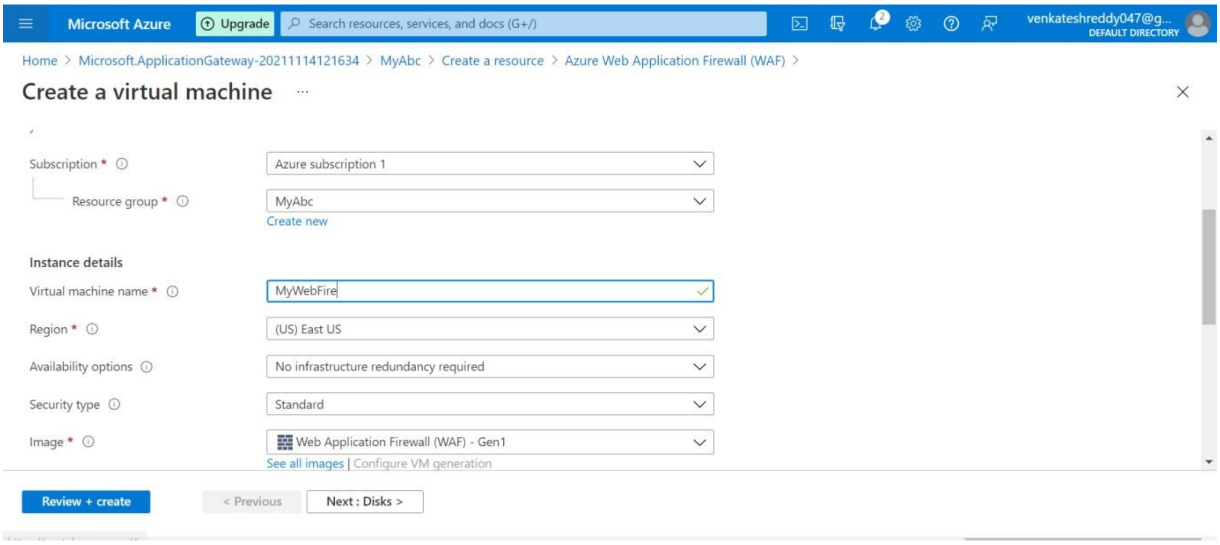
Want to deploy programmatically? Get started

Try out our "TEST DRIVE" for a complete Web application security testing environment. This is what our customers say:

"The ALB-X is intuitive and incredibly easy to use, we had it set up, configured and running in minutes."
"The ALB-X is brilliant. From testing to implementation and going live, it has exceeded our expectations & delivered."

Web Application Firewall (WAF) Features:

The Application Firewall controls the input, output and access to and from an application by inspecting the HTTP conversation between the application and clients according to a set of rules.


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
venkateshreddy047@g...
DEFAULT DIRECTORY
Home > Microsoft.ApplicationGateway-20211114121634 > MyAbc > Create a resource > Azure Web Application Firewall (WAF) >
Create new
See all images | Configure VM generation
Review + create
< Previous
Next : Disks >

Create a virtual machine

Subscription *: Azure subscription 1

Resource group *: MyAbc

Instance details

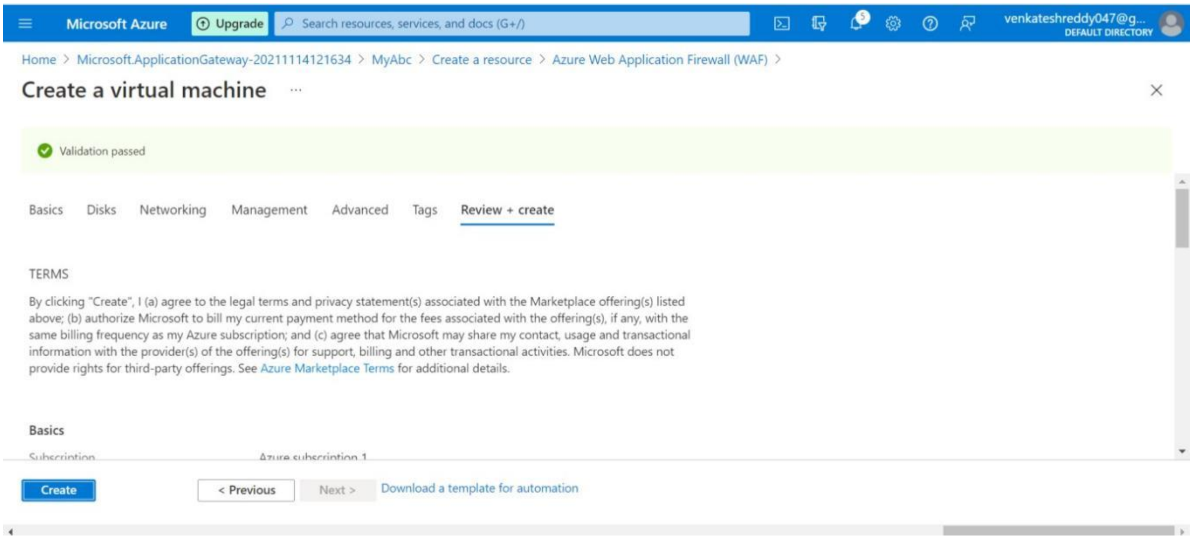
Virtual machine name *: MyWebFire

Region *: (US) East US

Availability options: No infrastructure redundancy required

Security type: Standard

Image *: Web Application Firewall (WAF) - Gen1


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
venkateshreddy047@g...
DEFAULT DIRECTORY
Home > Microsoft.ApplicationGateway-20211114121634 > MyAbc > Create a resource > Azure Web Application Firewall (WAF) >
Basics
Disks
Networking
Management
Advanced
Tags
Review + create
Create
< Previous
Next >
Download a template for automation

Create a virtual machine

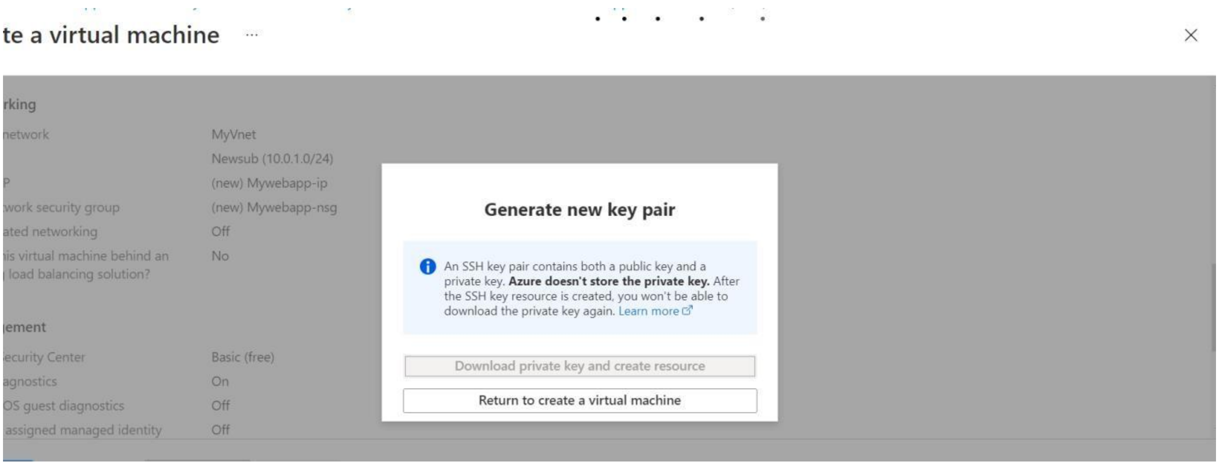
Validation passed

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), if any, with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See Azure Marketplace Terms for additional details.

Basics

Subscription: Azure subscription 1



te a virtual machine ···

rking

network	MyVnet
	Newsub (10.0.1.0/24)
P	(new) Mywebapp-ip
work security group	(new) Mywebapp-nsg
ated networking	Off
is virtual machine behind an load balancing solution?	No

ement

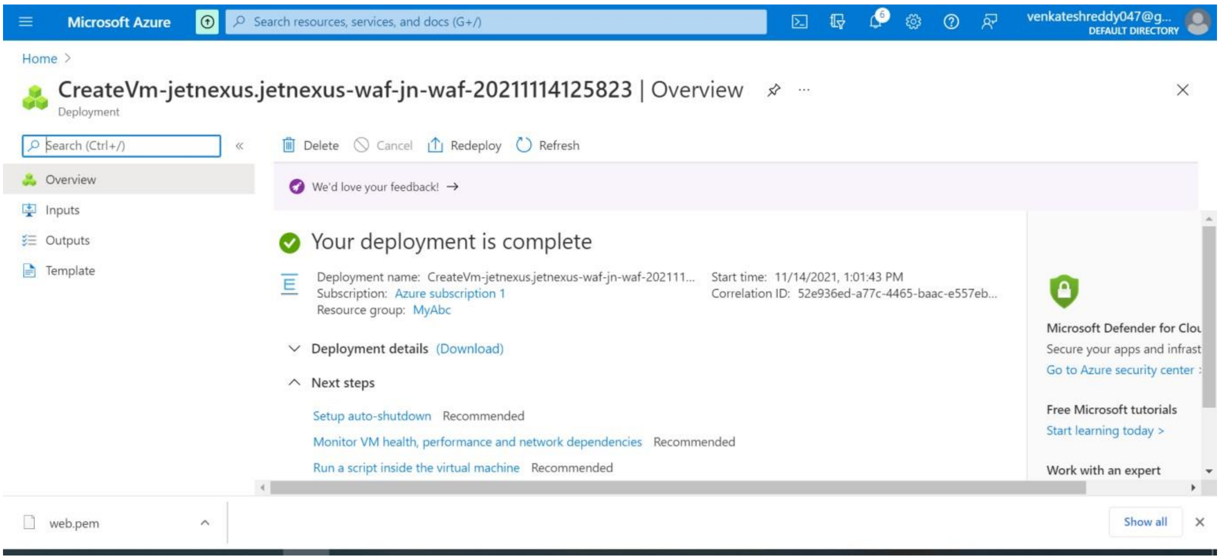
ecurity Center	Basic (free)
agnostics	On
OS guest diagnostics	Off
assigned managed identity	Off

Generate new key pair

An SSH key pair contains both a public key and a private key. **Azure doesn't store the private key.** After the SSH key resource is created, you won't be able to download the private key again. Learn more

Download private key and create resource
Return to create a virtual machine

Select / Remove Profile / Group: By default, all options in configuration help are enabled as well as advanced policy configuration options are disabled. By promoting advanced command processing, you can select a command / group command based on the application.



CreateVm-jetnexus.jetnexus-waf-jn-waf-20211114125823 | Overview

Deployment

Your deployment is complete

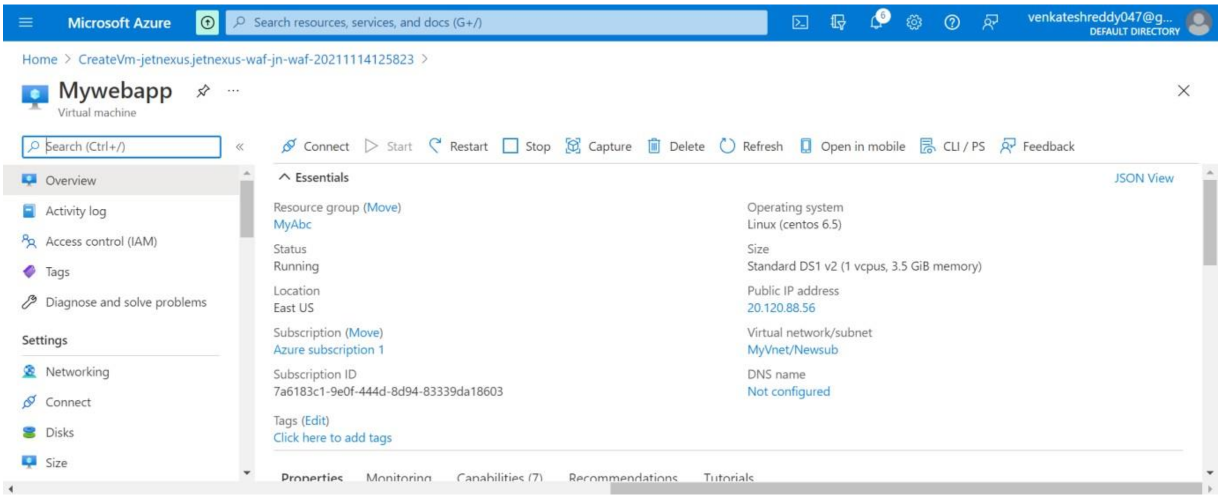
Deployment name: CreateVm-jetnexus.jetnexus-waf-jn-waf-202111...
Subscription: Azure subscription 1
Resource group: MyAbc
Start time: 11/14/2021, 1:01:43 PM
Correlation ID: 52e936ed-a77c-4465-baac-e557eb...

Deployment details (Download)

Next steps

Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended

Microsoft Defender for Clou
Secure your apps and infrast
Go to Azure security center
Free Microsoft tutorials
Start learning today >
Work with an expert
web.pem
Show all



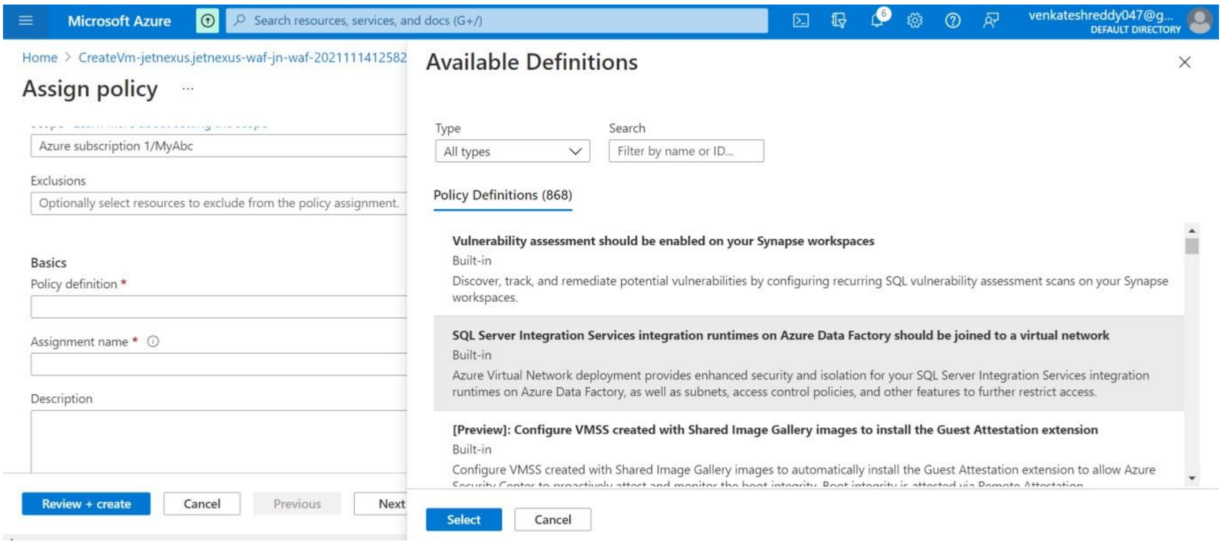
Microsoft Azure
Search resources, services, and docs (G+/)
venkateshreddy047@g...
DEFAULT DIRECTORY
Home > CreateVm-jetnexus.jetnexus-waf-jn-waf-20211114125823 >

Mywebapp

Virtual machine

Resource group (Move) MyAbc	Operating system Linux (centos 6.5)
Status Running	Size Standard DS1 v2 (1 vcpus, 3.5 GiB memory)
Location East US	Public IP address 20.120.88.56
Subscription (Move) Azure subscription 1	Virtual network/subnet MyVnet/Newsub
Subscription ID 7a6183c1-9e0f-444d-8d94-83339da18603	DNS name Not configured
Tags (Edit) Click here to add tags	

To set customized rules: A WAF administrator can write customized rules that have a legal name, legal need, and a number of relevant terms. These rules have higher requirements than other rules and regulations regulated by them. Depending on the relevant criteria, the customs law prohibits or allows traffic.



Azure subscription 1/MyAbc

Exclusions: Optionally select resources to exclude from the policy assignment.

Basics

Policy definition *

Assignment name *

Description

Available Definitions

Type: All types

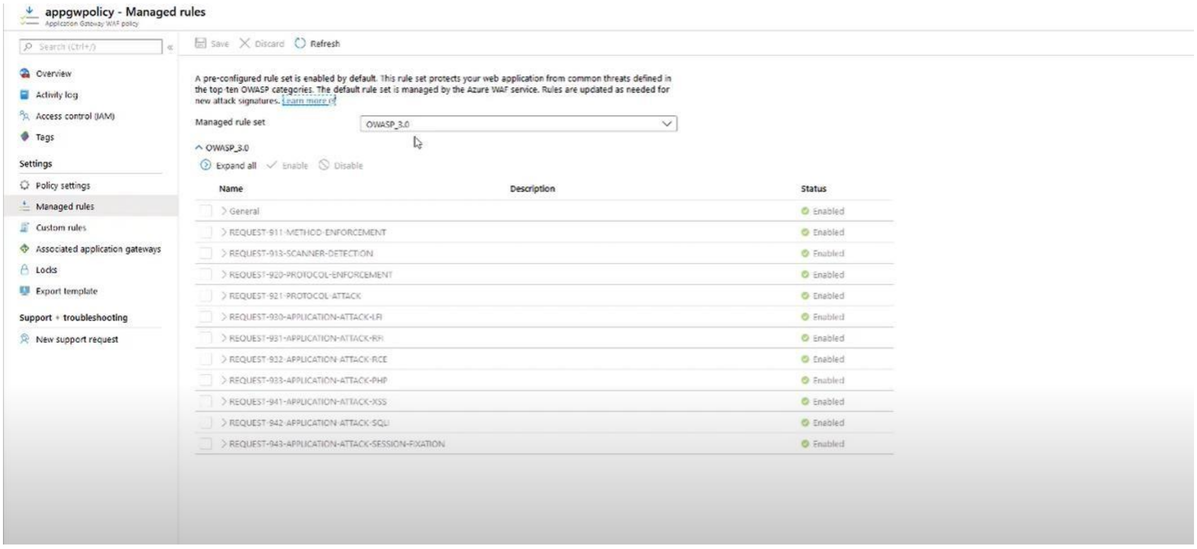
Search: Filter by name or ID...

Policy Definitions (868)

Vulnerability assessment should be enabled on your Synapse workspaces
Built-in
Discover, track, and remediate potential vulnerabilities by configuring recurring SQL vulnerability assessment scans on your Synapse workspaces.

SQL Server Integration Services integration runtimes on Azure Data Factory should be joined to a virtual network
Built-in
Azure Virtual Network deployment provides enhanced security and isolation for your SQL Server Integration Services integration runtimes on Azure Data Factory, as well as subnets, access control policies, and other features to further restrict access.

[Preview]: Configure VMSS created with Shared Image Gallery images to install the Guest Attestation extension
Built-in
Configure VMSS created with Shared Image Gallery images to automatically install the Guest Attestation extension to allow Azure Security Center to proactively attest and monitor the boot integrity. Boot integrity is attested via Remote Attestation

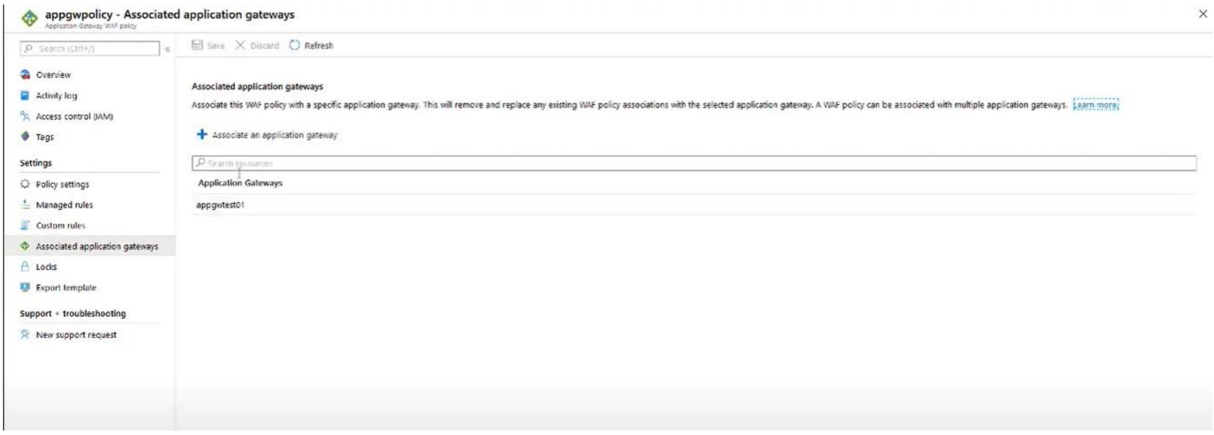


A pre-configured rule set is enabled by default. This rule set protects your web application from common threats defined in the top ten OWASP categories. The default rule set is managed by the Azure WAF service. Rules are updated as needed for new attack signatures. Learn more

Managed rule set: OWASP_3.0

OWASP_3.0

Name	Description	Status
General		Enabled
REQUEST-911-METHOD-ENFORCEMENT		Enabled
REQUEST-913-SCANNER-DETECTION		Enabled
REQUEST-920-PROTOCOL-ENFORCEMENT		Enabled
REQUEST-921-PROTOCOL-ATTACK		Enabled
REQUEST-930-APPLICATION-ATTACK-LFI		Enabled
REQUEST-931-APPLICATION-ATTACK-RFI		Enabled
REQUEST-932-APPLICATION-ATTACK-RCE		Enabled
REQUEST-933-APPLICATION-ATTACK-PHP		Enabled
REQUEST-941-APPLICATION-ATTACK-XSS		Enabled
REQUEST-942-APPLICATION-ATTACK-SQLI		Enabled
REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION		Enabled



Associated application gateways

Associate this WAF policy with a specific application gateway. This will remove and replace any existing WAF policy associations with the selected application gateway. A WAF policy can be associated with multiple application gateways. Learn more

Application Gateways
appgwtest01

WAF monitoring

To see more information about WAF policies, you must first activate the Diagnostic Logs, which you do by adding clinics. There are three options for storing logs:

- Keep the account
- Event hub
- Azure Monitor engine

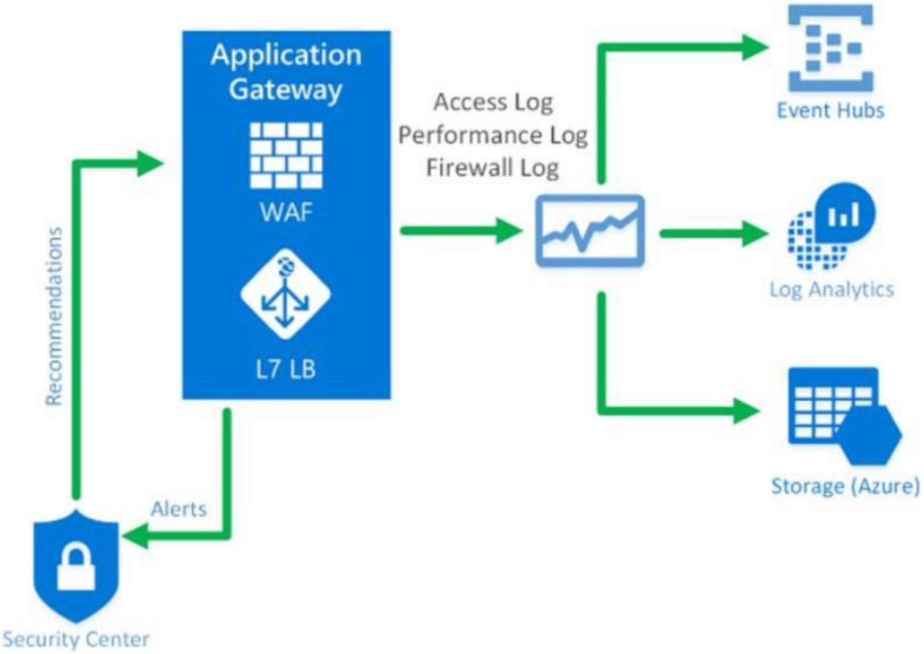


Figure 5: WAF monitoring

Now on the WAF open screen, you can view the file using Azure Storage Explorer. The Gateway application stores records under box 3:

- understanding-logs-applicationgatewayaccesslog
- understand-logs-applicationgatewayfirewalllog
- understand-logs-applicationgatewayperformancelog

The WAF database is a logical application log application. In the check box, type PT1H.json. This information is determined by a firewall created by WAF.

To test the process, a web firewall was created and used with all the steps and procedures shown in Figure, used in php, the system was used for 50 hosting servers, each as a joint venture, running various attacks from different users. The system has successfully prevented attacks against multiple users after detecting and distributing them to all physically connectedusers, and the system can detect attacks such as (xss, Ddos, sql injection). And it is before all the threats have been mentioned before. After blocking the attacker's IP address, the same attacker blocks additional attacks on different users. All users of electrical equipment worked equally before receiving the strike, and we can use wheel brake synchronization and distribution procedures to ensure the safety of different members on different networks and the security of web applications stored on different servers and platforms this is easy to use.

Evaluation

Most companies are comfortable with financial protection. According to a 2006 CSI / FBI survey, "97% of the companies surveyed administered vaccines, 98% were network-connected, 69% were affected. However,65% of these organizations' spyware is under attack, 32% have access to its internal information, and even 15% have avoided network interference "Two methods are widely used to prevent attacks. These must be understood and seen. Protection is the" first line of defence " The function of protection usually works to isolate certain users from the activities of the base - seeing them as dangerous or unworthy, but the conflict serves to identify protest attempts that go beyond the scope of the conflict. These models can be compared to secure data sources for malicious behavior (similar to the development of most viruses), orsome heuristics that identify the nature of the problem.

Unfortunately, the change was made by heuristic solutions at the cost of issuing false alarms to the contrary but without affecting the situation. The system's ability to detect unknown (unknown) attack patterns is often modified for many legitimate users. declared the victim. In the sensitivity of such a system, the number of false positives increases, making it impossible for them to act on their own (i.e., block some people). As a result, these reports are often sent to human observers for decision. On the other hand, a lack of understanding, which would allow human observation to disappear, would lead to real attacks that had never been seen before. On the security of website applications, it should be noted that this is multi-purpose. It includes security architecture and data management, security operations, and security of external systems and libraries used by applications (such as external data). Many experts, including Microsoft, think that they are changing security as a process that not only works on the life of the application, but in reality, it is rare.

This raises the importance of specific solutions to security issues, including those that are understood and addressed by project managers in organizations. Like Web Application Firewall (WAF)is probably a global solution that limits the risk of using applications, but is not infrequently used. This can be due to several reasons: - Difficulties in setting up WAF - which requires all aspects of user-to-user communication and application protection - Restrictions passed by the user, logic of the page process, etc. - Repeat the protection rules to be observed in the application. This means that it can be accepted that the application will notbe secure. - As the use of the site grows and evolves to interact with the new Terms of Use, the review of the WAF policies will continue. The combination of these conditions, especially the need for constant changes from WAF to mirror changes to the application, theoretically makes application developers generally responsible for the work - at least by the management organization. However, this leads to the situation that they have too many functions, which only means that the underlying tasks (applications) are not secure. Of course, their reaction increases the control that the WAF doesn't really need and it is better to promote the available resources for quality and efficiency. The authors 'personal experience recognizes that WAF approval is minimal in the business environment, especially for critical systems such as Internet marketing.

Framework of vulnerabilities threats and safeguard

Due to the content of vulnerabilities, threats and vulnerabilities the system is useful for developing new strategies for creating network security. Weaknesses or anomalies in the network that can compromise security. Results can be extracted from weak passwords, software viruses, computer viruses or scripts, virus free and SQL injection. A threat is an incident or occurrence that could endanger security. Threats are often used by the weak. Safety is a process in which the risk of one or all of the other factors is reduced. Security makes fear more or less important. These are also called blockchains and are administered blockchain. This vulnerability, threat and vulnerability system is useful for security assessment and experimental testing that maintains deployment and execution procedures. It is therefore related to the principle shown in Figure, which shows vulnerability as V and threat as T based on protection. According to S. Ka, at this point the expression frame is seen as the box in the box on the computer system. In its structure and management. In contrast, the outside of the box is a threat (T), including authorized personnel. In addition, an environment is a program that runs on configuration. This tutorial describes how the system works to protect our bodies when we think of an S1 agent against a T1 threat that tries to attack V1 with a weak S2 anti-T2 agent that tries ịwakpoV2. Eventually, S3 and S4 represent distorted areas, preventing other threats that use the weaker force of the requirement.

By accessing the system, users can access all the information they do not have or are restricted from accessing, depending on the purpose of the application. However, the excellent characteristics of SQL queries and knowledge of the communication patterns of others between the application process and the database process have allowed them to controlthe exchange. This requires unauthorized access to the system, bypass authentication mechanisms, and unauthorized access. manipulating data in the background database using no inputs (providing user feedback on such application data) without having to enter the system or not have access to evidence. This is possible because the system developer trusts the end user by ignoring the threat of security, doing it, and sending feedback to the user when creating the message. query that makes users request. Questions that accept user specific information and are referred to an application for data return to operation without a security check are considered invalid and may result in SQL injection.

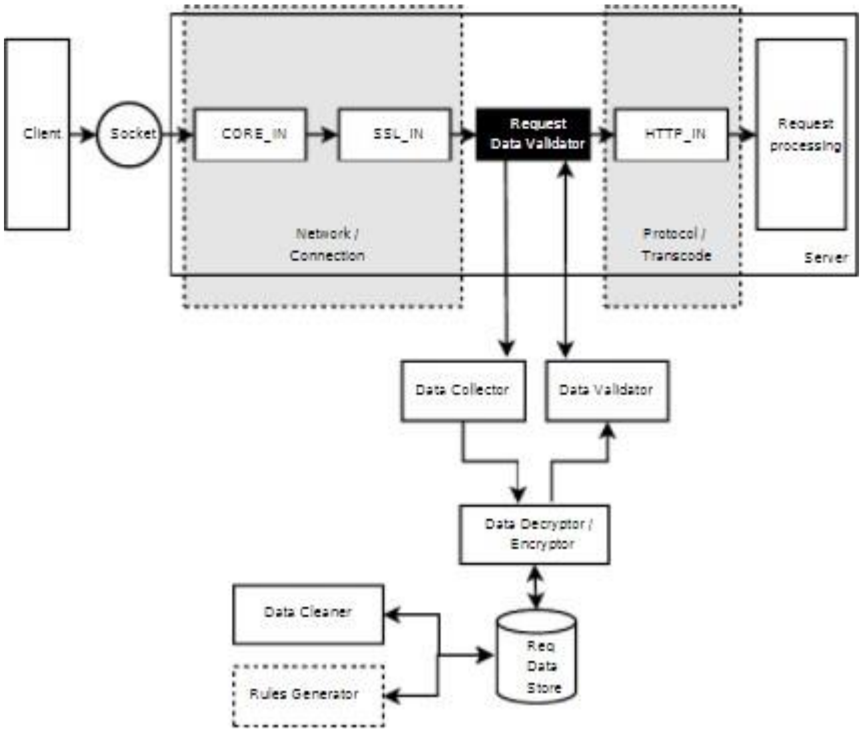


Figure 6: WAF components

9. Results & Analysis

Azure Web Application Firewall (WAF) from Microsoft provides central security for Azure Content Delivery Network (CDN) websites. WAF protects your web services from repeated use and abuse. Jobs are also available for senior staff and assisted as required.WAF and Azure CDN are global and mid-range solutions. It has been deployed worldwide in the Azurenetwork area. The WAF will stop the vicious attack near the base of the attack before they reach your site. You get world-class security at the highest level without interruption.The WAF policy quickly connects to each CDN at the end of registration. New rules can be submitted in minutes, so you can respond quickly to changed threats.

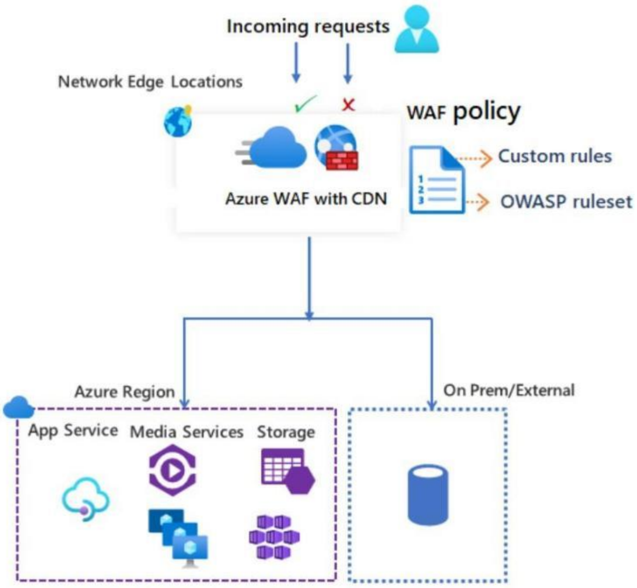


Figure 7: Azure WAF CDN

WAFs are not new. They have been on the market for many years and many manufacturers (e.g., Cisco, Barracuda, F5) are testing their hardware / software productsfor a large list of model comparison restrictions). There is also an open Apache Mod Security project that can be used to perform these tasks. However, all of these solutions are based on static rules - these must be declared manually for individual applications. Vendors typically provide templates for custom services, but custom applications often require more manual setup and regular maintenance, as previously described in implementation part. On the other hand, business solutions also have additional features, especially those that include medical devices, e.g., load measurement, etc. SSL support, etc.

The educational process must be completed; That is, it includes all types of applications - and because all of this work has to be done by staff, there are additional costs involved. However, because most commercial applications in web applications include usability metrics — which typically cover all applications— this also applies to WAF applications. Again, such changes in the business environment often indicate certain diagnostics that can be used for this purpose.

In short, this is a favourite of business leaders, especially in the infrequently changing web applications (such as Internet Banking). Using efficient web services, such as an Internet portal, can be difficult. The CL WAF provides less protection due to very low manual use. In this case, as described above, the data is collected by the user-supplied machine at a specifiedtime and flows continuously. The data in the last window is used to correct the revenue. The main problems arising from this situation are as follows:

- WAF only accepts values that correspond to end-user behavior. If these standards change over time, the WAF will receive more negative warnings
- The missile is specifically designed to focus on the educational process (e.g., bad data changes slowly over time). to be accepted by the WAF as a valid example).

10. Conclusion

To address the problem of latency and BFP, which typically governs WAF routing, this article describes the concept of an in-line and out-of-band, complex relationship that can select a traffic line type and location to continue in out-of-focus mode. By using this model, itnot only avoids late and inconvenient user interference, but also improves your response by allowing you to install more things. WAF Services supplements work together to define and identify traffic. Using open-source tools, any organization can follow design standards to improve the protection of its users and enhance the experience on its platform. In a rapidly changing world where technology is related to infrastructure, the importance of this document is to inform people of the importance of the cyber world as security. Informatics is not a vulnerability study to understand that we are not surrounded by technology. Technologyis all around us. The most important information! We are all aware of some cyber-attacks thatsteal our data, money and everything. We also know how technology affects people. The technology is applied. These applications will try to develop some methods that can help withsecurity. This article provides a detailed overview of some aspects of cyber security to help the reader take sensible steps. I also came here with great confidence because I think the process should be provided to the staff. However, I refused to use technological language because I was trying to reach a wider audience and not a place.

Network technology and usage are changing rapidly, and network security is difficult to achieve. Torgils are a source of many computer security threats and aggravate others. Security includes connecting to a secure network and repeating. Although network technology is on the rise, it is not surprising that people are increasingly using network security. This article describes some network security issues and details about new vulnerability, threat, and protection procedures. In our future work, our goal is to implement this framework in a real network with different scenarios.Processes for centralizing network walls Improve the process of tracking and protecting a website based on attacks by working with independent standard web walls as a seamless integration, easily transmitting and distributing attacks across all attached walls. in the system. Although every firewall site has its own attacks and can work on its own, it improves performance and reduces the potential for attacks on all systems together. And has increased the ability to reduce and prevent a variety of attacks.

The application of science and other biological techniques to the benefits of computer security has recently increased the attractiveness of scientists, and as cyber-attack experiments become more and more sophisticated, this is one way to solve these problems. The obvious advantage of such a WAF is that it has very little setup time due to the large amount of malicious content introduced into the web application.Of course, WAF is not new. They have been in the market for many years and many vendors (such as Cisco, Barracuda, F5) offer their hardware / applications (several lists of business models can be found). Thereis also an open-source Apache ModSecurityproject that can be used to provide these features. However, all of these answers are based on a complex process that must be manually customized for the website application. Vendors often provide a sample for a service or application, but if you want to offer an app, it usually requires a lot of manual and full-time configuration, as described earlier in this document. On the other hand, industrial solutions, especially those involving hardware manufacturers, have other characteristics, such as. size, SSL support etc,.

11futurescope:

The future scope of Web Application Firewalls (WAFs) in cybersecurity is promising, given the evolving nature of threats and the increasing reliance on web applications. Here are some key areas where WAFs are likely to advance and expand:

1. Integration with Advanced Threat Intelligence

Real-time Updates: Enhanced integration with threat intelligence feeds to provide real-time updates on emerging threats and vulnerabilities.

Automated Threat Responses: The use of automated responses based on the latest intelligence to quickly mitigate new attack vectors.

2. Artificial Intelligence and Machine Learning

Improved Anomaly Detection: Advanced machine learning algorithms for better anomaly detection, reducing false positives, and identifying sophisticated attack patterns.

Adaptive Learning: Systems that continually learn from new data to improve detection capabilities without manual rule updates.

3. Behavioral Analytics

User and Entity Behavior Analytics (UEBA): Incorporating UEBA to analyze patterns of user behavior and detect anomalies that might indicate compromised accounts or insider threats.

Contextual Awareness: Enhanced contextual understanding of user interactions with web applications to more accurately distinguish between legitimate and malicious activities.

4. Automation and Orchestration

Automated Configuration and Tuning: Tools that automatically configure and fine-tune WAF settings based on the specific needs of the web application and its traffic patterns.

Integration with Security Orchestration, Automation, and Response (SOAR): WAFs becoming part of broader security frameworks that automate the incident response process.

5. Cloud-Native and Serverless Architectures

Cloud Integration: WAF solutions designed specifically for cloud environments, offering seamless integration with cloud-native applications and services.

Serverless Security: Adapting WAF technologies to protect serverless applications, ensuring security in increasingly popular serverless architectures.

6. Comprehensive API Security

API Protection: Enhanced focus on securing APIs, which are becoming critical as more applications rely on microservices and interconnected services.

API Gateway Integration: WAFs integrating with API gateways to provide comprehensive security for API traffic.

7. Zero Trust Architecture

Zero Trust Principles: Implementing zero trust security models where every request is authenticated and authorized, reducing the risk of lateral movement within networks.

Micro-Segmentation: Using WAFs to enforce micro-segmentation, limiting access and reducing the attack surface within web applications.

8. Enhanced DDoS Protection

Advanced DDoS Mitigation: Improved capabilities for detecting and mitigating sophisticated DDoS attacks, including multi-vector and application-layer attacks.

Scalable Solutions: Leveraging cloud infrastructure to provide scalable DDoS protection that can handle large volumes of traffic.

9. Privacy and Data Protection

Data Masking and Tokenization: Advanced techniques for data masking and tokenization to protect sensitive information from exposure.

Compliance Management: Enhanced features to ensure compliance with global data protection regulations such as GDPR, CCPA, and HIPAA.

10. User-Friendly Interfaces and Reporting

Simplified Management: More intuitive user interfaces for easier management and configuration of WAFs.

Advanced Reporting and Analytics: Improved reporting capabilities providing detailed insights into security events and trends.

11. Collaboration and Community Sharing

Threat Intelligence Sharing: Platforms for sharing threat intelligence and attack patterns within the security community to improve collective defenses.

Open Source Contributions: Increased contributions to and adoption of open source WAF technologies, fostering innovation and collaboration.

12. Quantum-Resistant Security

Preparing for Quantum Computing: Research and development into quantum-resistant algorithms to ensure WAFs can protect against future quantum computing threats.

The evolution of WAFs will be driven by the need to address new and more sophisticated threats, the adoption of modern application architectures, and the integration of advanced technologies like AI and machine learning. As web applications continue to grow in complexity and importance, WAFs will play a critical role in ensuring their security.

12.References

[1] M. Abdelhaq, R. Alsaqour, M. Al-Hubaishi, T. Alahdal and M. Uddin. 2014. The Impact of Resource Consumption Attack on Mobile Ad-hoc Network Routing. International Journal of Network Security. 16: 399-404.

[2] A. Herzog and N. Shahmehri. 2007. Usability and security of personal firewalls. In New Approaches for Security, Privacy and Trust in Complex Environments, Ed: Springer. pp. 37-48.

[3] Comer, D. E., 1995. Principles, protocols, and architecture. Internetworking with tcp/ip.

[4] C. Hunt. 2010. TCP/IP network administration: O'reilly.

[5] G. Fox. 2001. Peer-to-peer networks. Computing in Science and Engineering. 3: 75-77.

[6] C. Mahalakshmi and M. Ramaswamy. 2012. Data transfer strategy for multiple destination nodes in virtual private networks. Journal of Engineering & Applied Sciences. 7: 1372-1378.

[8] D. B. Chapman. 1992. Network (in) security through IP packet filtering. In: Proceedings of the 3rd UNIX Security Symposium.

[9] J.-Y. Le Boudec. 1992. The asynchronous transfer mode: a tutorial. Computer Networks and ISDN systems. 24: 279-309.

[10] J. G. Andrews, A. Ghosh and R. Muhamed. 2007. Fundamentals of WiMAX: understanding broadband wireless networking: Pearson Education.

[11] M. Uddin, A. A. Rehman, N. Uddin, J. Memon, R. Alsaqour and S. Kazi. 2013. Signature-based Multi-Layer Distributed Intrusion Detection System using Mobile Agents. International Journal of Network Security. 15: 79-87.

[12] M. Uddin, R. Alsaqour and M. Abdelhaq. 2013. Intrusion Detection System to Detect DDoS Attack in Gnutella Hybrid P2P Network. Indian Journal of Science and Technology. 6: 71-83.

[13] Krause, M. (Ed.). (2006). Information Security Management Handbook on CD-ROM (Vol. 27). CRC Press.

[14] P. Qianwei. 2002. The crisis of and safeguard for network information environment [J]. Researches in Library Science. 5: 017.

[15] Peterson, L. L., & Davie, B. S. (2007). Computer networks: a systems approach.Elsevier.

[16] R. C. Summers. 1997. Secure computing: threats and safeguards: McGraw-Hill, Inc.

[17] C.-X. Qi and Q.-D. Du. 2009. A Smart IVR system based on application gateways. In Hybrid Intelligent Systems. HIS'09. 9th International Conference on. pp. 110-115.

[18] S. Jajodia, S. Noel and B. O'Berry. 2005. Topological analysis of network attack vulnerability. In Managing Cyber Threats, Ed: Springer. pp. 247-266.

[19] W. R. Cheswick, S. M. Bellovin and A. D. Rubin. 2003. Firewalls and Internet security: repelling the wily hacke. Addison-Wesley Longman Publishing Co., Inc.

[20] Yee, D. (1999). Development, ethical trading and free software.

[21] Z.-L. Zhang, Y. Wang, D. H. Du and D. Shu. 2000. Video staging: a proxy-server-based approach to end-to-end video delivery over wide-area networks. IEEE/ACM Transactions on Networking (TON). 8: 429-442.

[22] Messmer, E., 2013. Gartner: Cloud-based security as a service set to take off. Network World.

[23] Amirtahmasebi, K., Jalalinia, S. R., &Khadem, S. (2009, November). A survey of SQL injection defense mechanisms. In 2009 International Conference for Internet Technology and Secured Transactions,(ICITST) (pp. 1-8). IEEE.

[24] Halfond, W. G., &Orso, A. (2007, September). Improving test case generation for web applications using automated interface discovery. In Proceedings of the the 6th joint meeting of the European software engineering conference and the ACM SIGSOFT symposium on The foundations of software engineering (pp. 145-154).

[25] Djuric, Z. (2013 September). A black-box testing tool for detecting SQL injection vulnerabilities. In 2013 Second international conference on informatics & applications (ICIA) (pp. 216-221). IEEE.

[26]A. Sari, "Countrywide virtual siege in the new era of cyberwarfare: remedies from the cyber-firewall: Seddulbahir," *Journal of Cyber Security Technology*, vol. 2, no. 1, pp. 14–36, Jan. 2018, doi: 10.1080/23742917.2018.1476956.

[27]M. Sekuloski, "Security Sector Reform Wisdom for Cyber Security Institution Building: The Case of Serbia," *Information & Security: An International Journal*, vol. 34, pp. 69–90, 2016, doi: 10.11610/isij.3406.

[28]A. Muzakka, B. Sugiantoro, and Y. Prayudi, "PEMANFAATAN HASIL REPORT NEXT-GENERATION FIREWALL SEBAGAI SECURITY AWARENESS," *Cyber Security dan Forensik Digital*, vol. 2, no. 2, pp. 69–76, Nov. 2019, doi: 10.14421/csecurity.2019.2.2.1600.