Table of Contents

ACKNOWLEDGEMENT

It was a wonderful journey of my onsite internship. I was lucky to get chance to work in such a great company under excellent guidance of Kandarp Sir at Indusface. It was wonderful to work under friendly seniors and it wouldn’t be as fun without being the part of the organization. I would like to thank Assistant Professor Madhav Ajwalia to support me in my journey as our internal guide. We gained valuable skills and knowledge. We would also like to thank our HOD DR. Parth Shah. We heartily thank you for all your support. Thank you for motivating us and guiding us through the obstacles. Thank you for this memorable experience.

ABSTRACT

Cyber Security is a field that deals with security of various elements of an organization including applications, networks, hardware devices and much more. It includes of dealing with pentest the applications, networks to find different vulnerabilities and also includes defending them against various attacks and continuous monitoring and incident management. Indusface has developed two such products working past many years including a Web Application Scanner (WAS) and a Web Application Firewall (WAF) that they provide to clients as a managed service. It is completely integrated with cloud and also services like CDN to enable faster and better experience along with security.

It has various departments including a VAPT team that deals with manual penetration testing of applications, MSS teams that deals with continuous monitoring and also client support, Signature development team that deals with development of various rules and signatures of firewall and a development and sales team as well. As I was fresher, they guided me through their tools and technologies that they use to protect and defend against various cyber-attacks.

COMPANY INTRODUCTION

Indusface is a leading application security SaaS company that secures critical Web, Mobile, and API applications of 3000+ global customers using its award-winning fully managed platform that integrates web application scanner, web application firewall, DDoS & BOT Mitigation, CDN, and threat intelligence engine. Indusface has been funded by Tata Capital Growth Fund II, is the only vendor to be named Gartner Peer Insights™ Customers' Choice' in all the 7 segments for Web Application and API Protection Report 2022, is a "Great Place to Work" certified SaaS product company, is PCI, ISO27001, SOC 2, GDPR certified and has been the recipient of many prestigious start-up awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company, Deloitte Asia Top 100, among others.

CHAPTER 1:
UNDERDTAND THE PRODUCTS

1.1INTRODUCTION TO WAS:

WAS (Web Application Scanner) is an automated scanner that is used by security teams as a part of their security assessment and also to fortify their web application against any possible vulnerabilities. This scanners are quite capable of detecting most of the vulnerabilities but still automated scans have their own advantages and disadvantages.

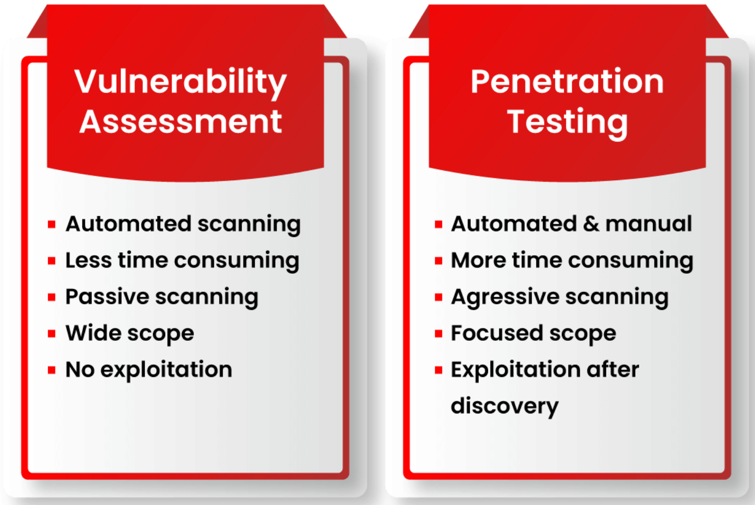


Figure 1.1 Comparison of auto & manual scan

As shown in above figure, automated scanning that is vulnerability assessment has its own utilities while pentesting is important equally. But the reports obtained from these automated scanners are quite helpful for penetration testing as it helps to scope out the targets and also possibilities of manual findings.

1.1.1 Scanner as a Service

There are many companies who instead of providing it as a product, gives scanner as a service to required clients. They have various kinds of plans or subscriptions as per the client requirements for their security. Services in scanner can include Malware Scanning, Vulnerability Management, Policy compliance of their application and much more. Also, such platforms are now integrated with cloud platforms and also services like CDN to offer a better performance along with security.

Companies rely such automated scanners as a part of their security assessment and also to meet various compliance policies that is mandatory for their organization to follow.

1.2 INTRODUCTION TO WAF:

A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defense, and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors.

By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine’s identity by using an intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server.

1.2.1 Protection against attacks

A WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy modification can be implemented, allowing for faster response to varying attack vectors; during a DDoS attack, rate limiting can be quickly implemented by modifying WAF policies.

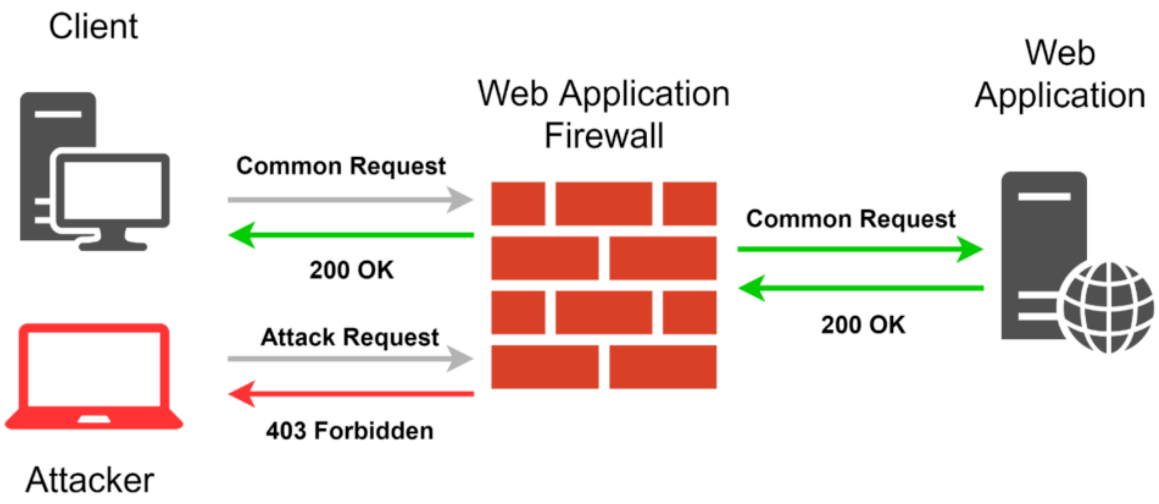


Figure 1.2.1: WAF working

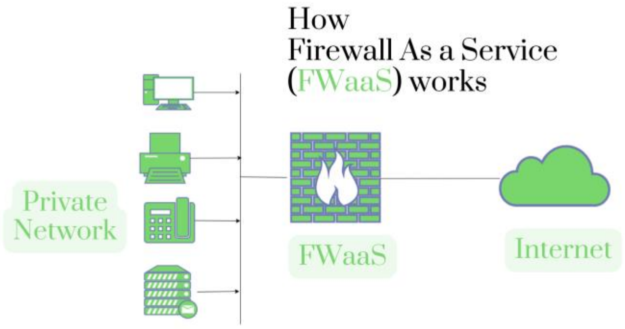
1.2.2 How it is managed

Many companies instead of providing firewall just as a product to their clients gives managed services where they manage complete firewall as a service as per client requirements. Many a times, it may happen that the person from security may be or not be completely familiar with new firewall, its working and rules generation and management.

Firewall as a Service filters network traffic to safeguard organizations from both inside and outside threats. Along with stateful firewall features such as packet filtering, network monitoring, Internet Protocol security (IPsec), secure sockets layer virtual private network (SSL VPN) support, and Internet Protocol (IP) mapping features, FWaaS also has deeper content inspection capabilities that include the ability to identify malware attacks and other threats. FWaaS is positioned between your network and the internet. As traffic attempts to enter your network, the FWaaS solution inspects it to detect and address threats. The inspection analyzes the information contained in the header of each data packet, garnering insight into where the packet came from and other behaviors that may signal it is malicious.

So, in such scenarios companies have a separate team which takes care of applying the necessary rules for the application, generating custom rules are per the requirement of the security and also integrating this firewall with their SIEM (Security Information and Event Management) tool where complete flow of traffic is monitored, triaged and also rules are generated in that for incident management.

Also, managing such services that deals with a lots and lots of ongoing traffic across network with applications that are critical working on it, CDN is also one of the service that is integrated with it which is also managed by MSS Team. CDN helps in fast delivery of content and reduce latency to access resources for clients.

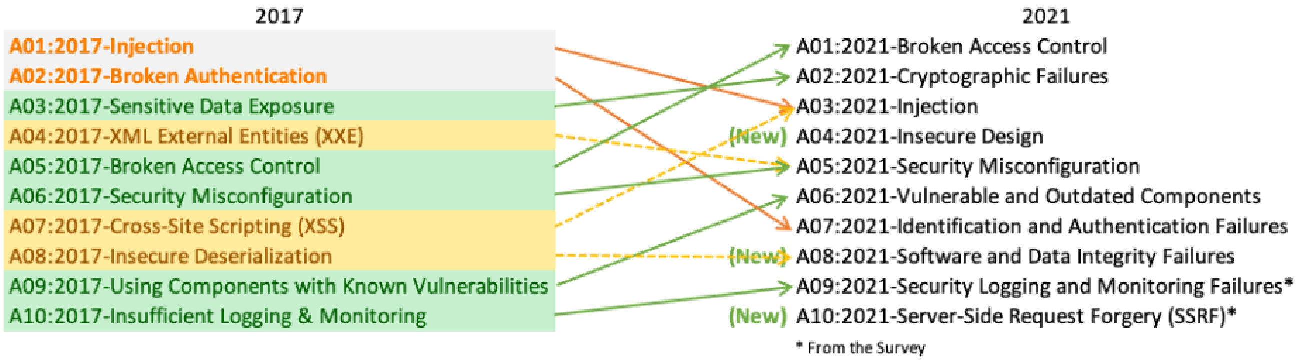


CHAPTER 2:

WAS (WEB APPLICATION SCANNER)

2.1WHY AUTOMATED SCANNERS ARE IMPORTANT?

Automate Web Application Scanners are implemented as a part of security measure by the organization's security team. Automated Scanners can include from a normal assessment of the application to complete vulnerability assessment. These scanners also come with features of scheduling the scans at some particular timelines because in many big organizations, there very strict security policies that must be followed and scanners play an important role in it.


2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

Web Applications top vulnerabilities are defined by OWASP Top 10. So, these automated scanners are designed and made in such a way that they just not only scan and disclose low and medium vulnerabilities but such high and critical are also important and also it is more necessary for the organization to implement security countermeasures against them.

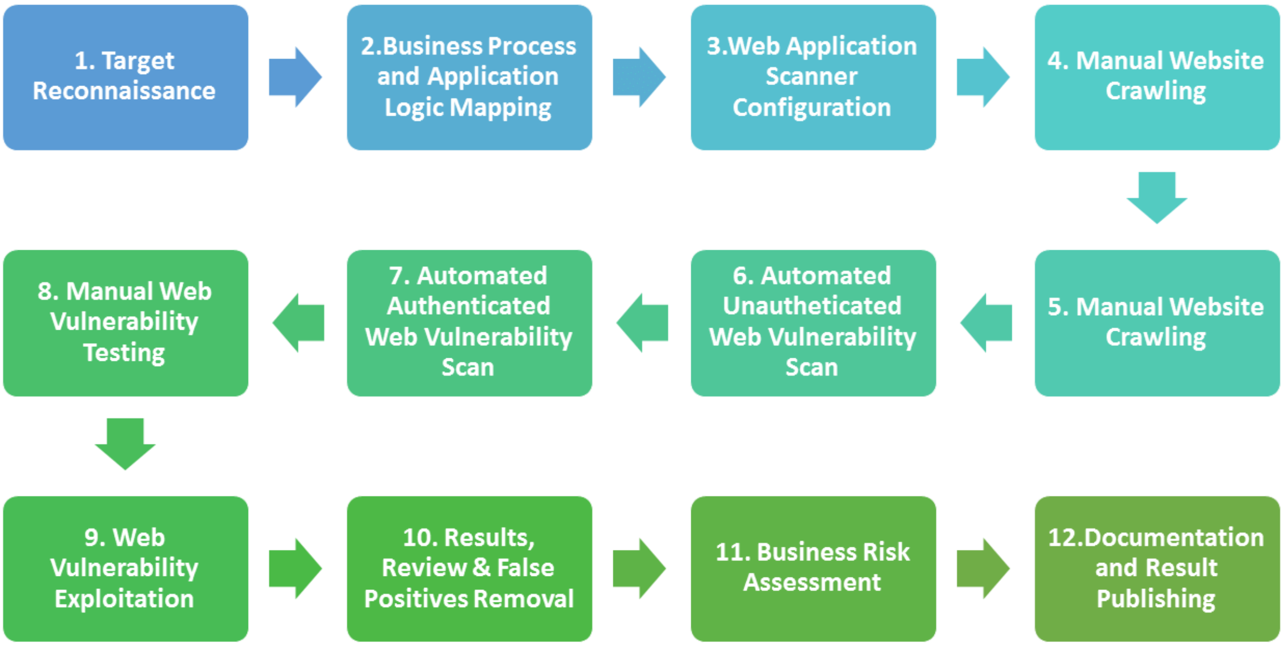
Also, malware monitoring that is important for an organization to check that whether any malicious activities are going on or any adversary is trying to attack, scanners also take care of that scan and report to it so that security team can track the issue down.

In IT security, there are various compliance policies that are needed to be followed. Many scanning services are capable to managing and applying those compliance policies so that it is certified to use and also trusted by everyone as those security policies are designed for user's security controls only. Policies like GDPR, DPA, and PCI DSS are some of the policies that are compiled by these scanning services. While monitoring such alerts and detection, there are high chances that due to some technical or logical error or change a false positive may be generated which needs to be taken care of by the security team through their monitoring platform.

2.2HOW IT IS IMPORTANT IN PENTESTING

While performing task of complete penetration testing, it is important for pentesters to decide the scope and limitation of finding vulnerabilities such that the business operations are not affected and also task can be carried out easily. When automated scanners are placed within an organization, the VAPT team takes results from these scanners as an asset that they will be testing it. Also, while documenting the POC of manual findings, the results from automated scanners are taken into consideration as many organizations as for both kind of findings.

In case of scanner provided as a service, the penetration testing task can be carried out by their team if client has requirements. These findings are also helpful when audit is being conducted for any organization describing their security parameters.



1. Target Reconnaissance
2.Business Process and Application Logic Mapping
3.Web Application Scanner Configuration
4. Manual Website Crawling
5. Manual Website Crawling
6. Automated Unauthenticated Web Vulnerability Scan
7. Automated Authenticated Web Vulnerability Scan
8. Manual Web Vulnerability Testing
9. Web Vulnerability Exploitation
10. Results, Review & False Positives Removal
11. Business Risk Assessment
12.Documentation and Result Publishing

Figure 2.2: Process of Assessment

Intruder works seamlessly with your technical environment to test your systems for security from the same perspective (the internet) as the people who are looking to compromise it, using industry leading penetration testing software (software used by penetration testers) under the hood. While there are a few options available for using online penetration testing tools, Intruder is designed to be simple and fast, so you can get set-up and protected in little to no time.

Intruder ensures that your systems are being continuously monitored for a spectrum of vulnerabilities, including web-layer security problems (such as SQL injection and cross-site scripting); infrastructure weaknesses (such as remote code execution flaws); and other security misconfigurations (such as weak encryption, and services that are unnecessarily exposed). A comprehensive list of all ~10,000 checks can be found in the Intruder portal.

CHAPTER 3:

WAF (WEB APPLICATION FIREWALL)

3.1 APPLICATION LAYER FIREWALL

An application firewall is a type of firewall that controls network access to, from or by an application or service. Such products monitor the use of applications and block any activities that don’t meet the configured policy of the firewall.

Application firewalls protect application communications in a similar manner that network firewalls secure network communications. Because they are aware of the languages applications use to transmit information, they can deny or modify invalid or suspicious activities—protecting organizations against attacks.

Application firewalls are generally designed to control all network traffic on any OSI layer up to the application layer. They differ from stateful network firewalls in that application firewalls can control network traffics regarding a specific application; whereas stateful network firewalls are not able to control traffic regarding a specific application.One type of application firewall is a web application firewall (WAF), which is specifically designed for HTTP applications. WAFs are expected to protect web applications from a few types of attacks, including injection attacks and application layer denial of service (DoS). They are generally deployed in from of web servers, protecting web apps from both internal and external threats.

Application firewalls can be active or passive.

Active – Active app firewalls actively inspect all incoming requests—including the actual message being exchanged—against known vulnerabilities such as SQL injections, parameter and cookie tampering, and cross-site scripting. Only requests deemed “clean” are passed to the application.

Passive – Passive app firewalls act in a similar way to an intrusion detection system (IDS) in that they also inspect all incoming requests against known vulnerabilities, but they don’t actively reject or deny those requests if a potential attack is discovered.

Application firewalls are generally remotely updateable, which allows them to prevent newly discovered vulnerabilities. They’re often more up to date than specific security-focused code included in applications, due to the longer development and testing cycles required to include such code within applications.

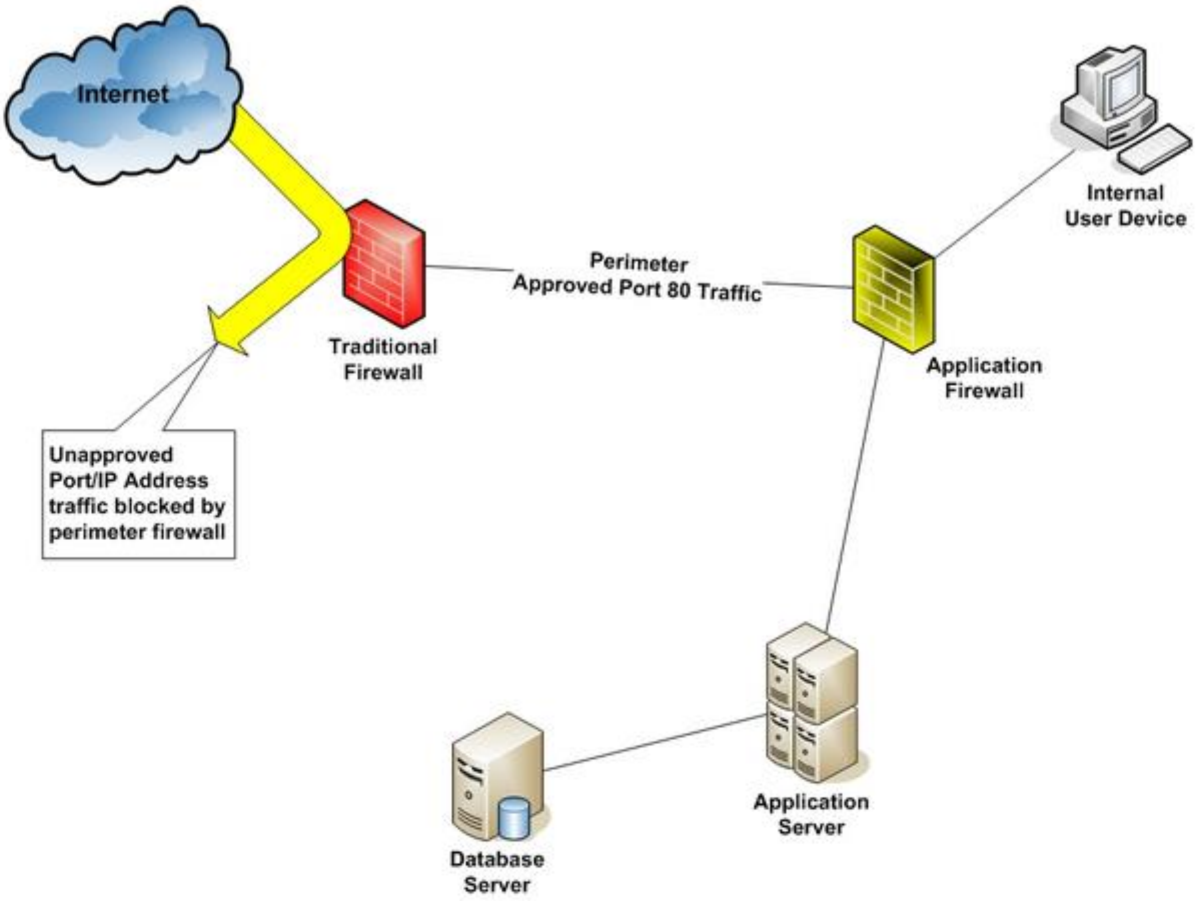


Figure 3.1 Firewall working

A WAF that operates based on a blocklist (negative security model) protects against known attacks. Think of a blocklist WAF as a club bouncer instructed to deny admittance to guests who don’t meet the dress code. Conversely, a WAF based on an allowlist (positive security model) only admits traffic that has been pre-approved. This is like the bouncer at an exclusive party, he or she only admits people who are on the list. Both blocklists and allowlists have their advantages and drawbacks, which is why many WAFs offer a hybrid security model, which implements both.

3.2 FIREWALL AS A SERVICE

FWaaS allows customers to partially or fully move security inspection to a cloud infrastructure. With security in the cloud, your solution is managed by the cloud provider, who will maintain the hardware infrastructure that powers your solution. Your service agreement will include details outlining the types of features you will have access to, depending on the subscription you choose. Many companies need a service-based architecture because it gives them the freedom to expand on-demand without having to worry about provisioning new hardware.

Maintaining hardware firewalls does not fit into many companies' budgets or operational workflow, making FWaaS an attractive option. The convenience that comes with all updates and adjustments to settings being handled by the provider allows organizations to free up critical resources, time, and energy for other, mission-critical pursuits.

With FWaaS, an organization's distributed sites and users are connected to a single, logical, global firewall with a unified application-aware security policy, allowing them to better scale security. The Firewall as a Service provider gives all employees access to resources that protect a wide range of devices, making FWaaS a one-solution-fits-all option, regardless of the size of the organization.

This makes FWaaS a foundational component of any secure access service edge (SASE) architecture because it provides the functionality of NGFW without the high capital expenditure (CapEx) costs associated with an on-premises wide-area network (WAN) infrastructure investment. In an on-premise setup, upgrading your system involves taking the time to source the best components and compare them with each other before committing to a purchase. Then, after parting with valuable funds to purchase the item, the organization has to ensure staff is familiar with how it operates, how to maintain it, and how to ensure it is properly updated. For many companies, this is a heavy load to lift. With FWaaS, this is all taken care of by the provider.

FWaaS takes advantage of advances in software and cloud technologies to deliver a wide range of network security and inspection capabilities, provided on-demand for users anywhere. With an in-house setup, your IT team has to keep abreast of the latest software and technological developments impacting the world of network security. Some companies need FWaaS simply to ensure they have the latest and greatest protection. When the provider protects your network, you are more likely to have cutting-edge technologies and methodologies than if you put that responsibility on your in-house staff.

Advantages of Firewall as a Service

For companies looking for an agile security solution, FWaaS presents several distinct advantages. To maintain flexibility, many organizations are shifting away from traditional in-house options and trusting an FWaaS provider with the protection of their network.

Unified Security Policy Deployed via the Cloud

Unified security involves combining multiple security initiatives under one umbrella. The overarching service is therefore able to shield the organization from a wider variety of threats. A unified security architecture may incorporate intentional redundancy that results from two or more security measures that are able to stop the same kind of threat.

Having this managed in the cloud streamlines your setup. Instead of having to find, purchase, configure, and manage each facet of your unified architecture, the service provider takes care of all that for you. Deploying an in-house solution can be complex and time-consuming. There are a lot of moving parts, equipment-related and otherwise. With an FWaaS, on the other hand, deployment is handled by the provider. Often, this can be done quickly and with little to no work on the part of the company. In situations where custom configurations are needed, the organization only has to provide the necessary information to the provider, who can then customize the deployment.

Your OpEx consumption model needs to have flexibility as well. It is rare that an organization’s OpEx figures are static—they need to be able to adjust as needs arise. With FWaaS, you can find ways to get the most out of your budget and even ways to limit OpEx expenditures while still achieving the security you need. You can present your situation to your FWaaS provider, and they can help you choose the package that suits your needs. This can change as frequently as you want with very little onboarding time.

CHAPTER 4:

TRAFFIC MONITORING

4.1 DIFFERENT PARAMETERS OF TRAFFIC MONITORING OF APPLICATION

Website traffic monitoring is primarily done to keep a record of website performance, stability and overall user experience. They key objective is to evaluate the website's performance from the end users' standpoint.

Some of the things that can be monitored in website traffic include:

- Number of users visiting the website within a specific time (hour/day/week)
- Overall visit length
- Most popular page or website component
- Website speed (page download speed or website access speed)
- Website bounce rate
- Popular visitor channels (referred by website or search engine)

Website traffic monitoring is generally followed by an ongoing reporting process to help improve the website's user experience and overall performance. Website traffic monitoring is also used in Internet marketing to analyze the type of visitors, customer demographics, popular content and to measure the success of marketing strategies, campaigns, sales, etc.

Monitoring network traffic provides immediate internal visibility into potential security and operational issues. For your system administrators, these key insights are crucial for making sure your network is well protected and performing as it should.

High spikes in network traffic are probably the first thing that your system administrators will examine. This is because high traffic spikes and traffic fluctuations are a dead giveaway for suspicious behavior that indicate a break-in by a hacker.

Malware outbreaks and hacking attempts, for example, cause spikes in network traffic when hackers use malware to force login to employee computers and devices.

Frequent scans are necessary to detect threats, such as undetected malware infections, data exfiltration, denial of service (DoS) attempts, unauthorized device access, and more.

For system administrators, some types of external misuse are much easier to find. Because the role of system administrators is to look at communications between devices, they can find indications of attacks based on previously detected attacks.

It becomes more challenging to find security events captured on the host device such as login attempts and virus detections. (Learn more on why secure remote access is important for businesses who have employees working remotely).

When company employees experience reduced internet speeds, it is usually an early indication of a security issue. At other times, traffic spikes are indications of operational issues such as speed. Because network speed is measured by throughput and bandwidth, businesses may find bandwidth monitoring and network usage tools extremely useful.

When it comes to finding the underlying issue of a slow network, monitoring network traffic and device performance go hand-in-hand. Simply, investing in additional bandwidth may be a quick fix — but the underlying issue will remain.

Instead, to address the cause of performance problems, system admins need to perform further inspection and analysis. In doing so, admins will typically be able to identify the applications that are withholding the most bandwidth and may require you to configure applications.

Businesses aren't reacting fast enough to malicious network activity. According to Cisco, the average time for detecting threats is 100-200 days. In 2019, the average time to identify a breach was 206 days.

This statistic should be alarming to businesses that currently have network firewalls deployed. Once a hacker is inside, it's hard to tell what they will do. With an extended period of time in which a hacker goes undetected when your network can mean greater losses for your company, whether it be the theft of sensitive company information or customer data leakage. Web analytics tools like Google Analytics allow you to track visitors, including whether they are new or returning visitors, how long their visit lasts, how they came to your site, etc.

A WAF analysis report, on the other hand, can easily and effectively track both legitimate and illegitimate visitors to your websites.

WAF reports will tell you where both legitimate and malicious visitors (i.e hackers) are coming from, essentially creating an analytics system that sorts the good traffic from the bad. This is because, with a WAF, you can block traffic by specific country and IP, giving you control over suspicious visitor activity on your website.

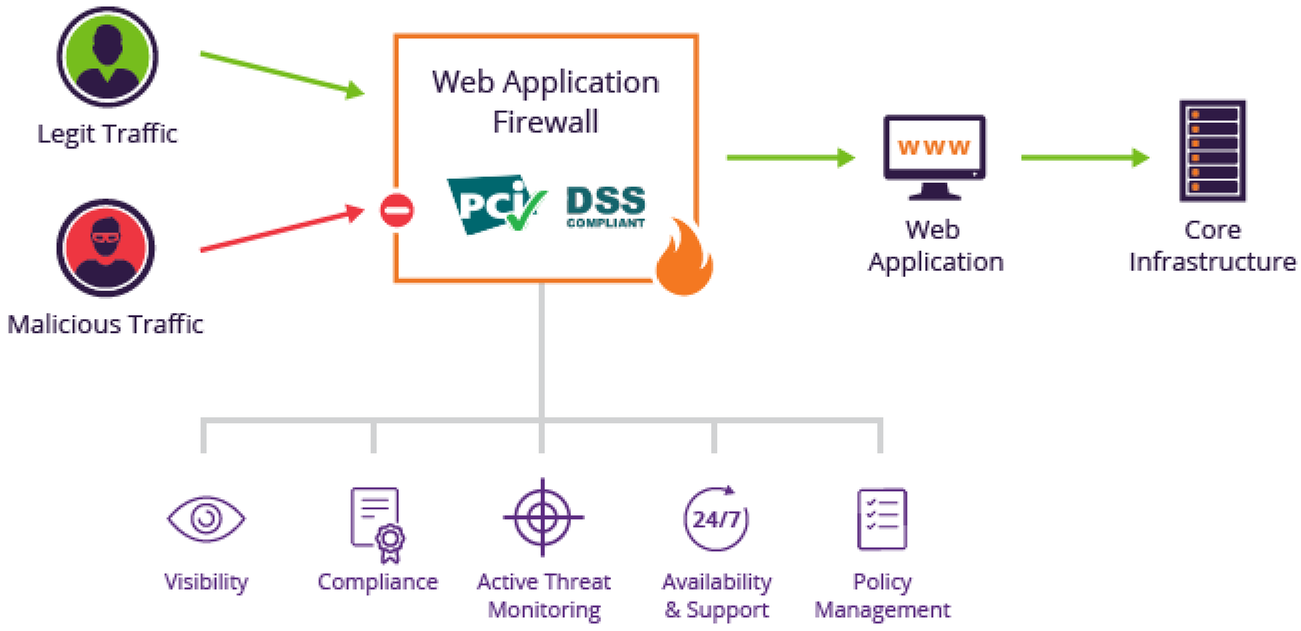


Figure 4: Traffic Analysis

Therefore, authentication and hack prevention is needed prior to granting access to users because, without it, an unknown visitor may have malicious intentions. The same can be said about web application firewalls. A good WAF should have the latest technologies to be able to accurately distinguish "good" and "bad" traffic to the web application. (Learn more about the different WAF technologies here).

Security monitoring is key to any healthy cybersecurity strategy. In today's cybersecurity climate, it's important for businesses that have the resources to actively pursue preventive measures.

CHAPTER 5:

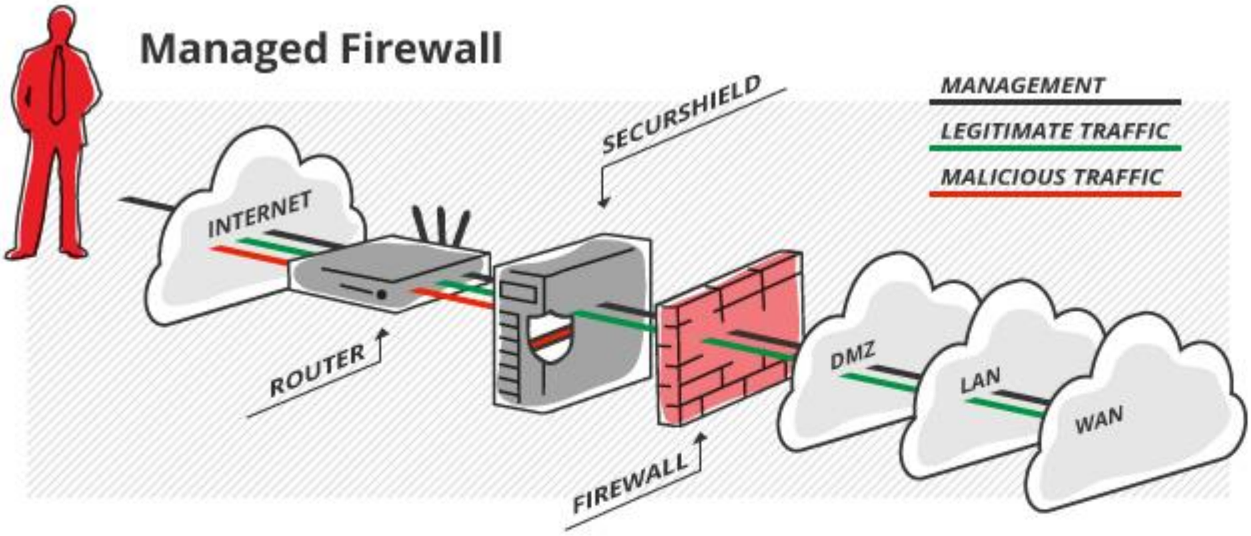
CLIENT QUERIES

5.1 TICKETS RAISED BY CLIENTS FOR QUERIES

In managed services there are many kind of queries raised by clients for firewalls as well as scanning services. As managed service, the first job of the team is to ensure 24x7 support as the clients can be from outside of the country as well and also the maintenance or the security scans undergo when the infrastructure is free to scan and the business is not affected. So, many a times queries arise like why they are not able to access their application, why they are not able to access it from internet and able to access from the intranet, why the response time of application has reduced, why CDN is not properly delivering the content to the client request and also queries related to scanning services like many a times there arises many false positives that make it difficult for the team to track and also tell the clients that the bug or the vulnerability detected by the scanner is not valid or false positive.

Benefits of Managed IT Services from Global Data Systems

- Strategic Managed IT: We help you solve your technology related business problems.
- Connectivity: We get you reliable, secure connectivity anywhere in the western hemisphere in 48 hours.
- Support: When you need help simply call our 24x7x365 support number.
- Billing: Instead of managing hundreds of vendors - get one, easy to read bill from GDS.



5.1.1 How the team responds to the queries?

When clients are not able to get any problem resolved, there is a ticketing system that is made to resolve and escalate such queries. Either JIRA or ZOHO is used to assign a ticket to an individual or the team and then complete tracking of that issue takes place based on the communication on the ticket generated.

ZOHO is mainly used as it is ease for clients as well and also the complete organization is able to manage and track the issues easily. When issues are resolved the tickets are closed and that is marked as complete and if that issue is raised further, then ticket is opened again and given a due date so that query can be resolved as soon as possible.

This is one of the important tasks in managed services as there are many potential clients like Financial Institutions, Government sites and applications, Educational and E-Commerce sites and platforms, and much more. So, the business should not be affected because of the query from the service or any technical fault from company side. That is why, the team is always is ready to respond and react to such incidents

CHAPTER 6:

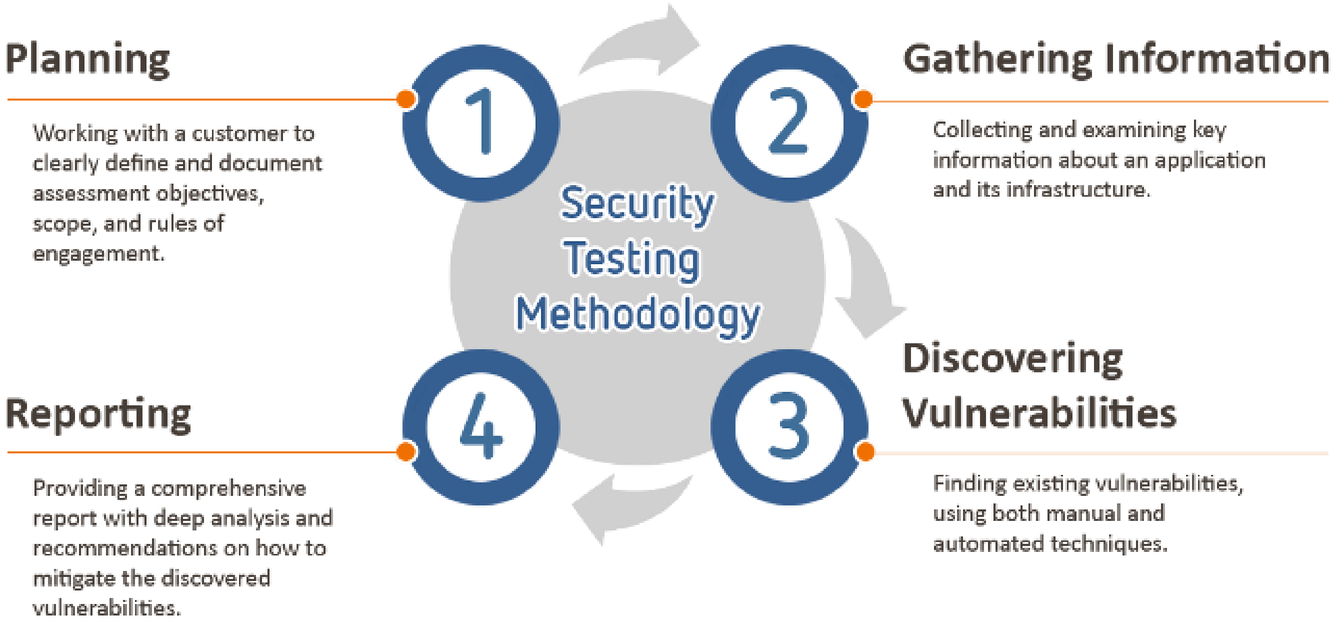
MANUAL AND AUTOMATED SCANS

6.1 HOW MANUAL AS WELL AS AUTOMATED TESTS ARE CONDUCTED

The automated approach sounds enticing that only requires a tool to be deployed that runs in your environment and generates the result for you. However, with vulnerability assessment for assessing the networks or the systems is doable with a tool such as Nessus, which is a well-known commercial tool in the security industry which we use in our engagements. It's plugins based tool which discovers vulnerabilities accordingly about the environment or the system.

But for penetration testing the same cannot be said mostly, tools automatically can exploit the vulnerabilities they find but till what extent; will it try Denial of Service (DoS) on the system or offer a reverse shell back of an exploited system; Will it be able to exploit the vulnerability if found, but the payload is being blocked by an endpoint; will it be able to identify the change in parameter and keep exploiting until it gets exploited?

Some downfalls of automated tools are to look out for is false positive running a tool which is improperly configured may or may not give the proper output that one expects. The worst-case scenario is the automated tool brings down the whole network or a critical system, which will not only halt the business but may cost them a lot of money due to downtime. Operating such tools also requires a knowledgeable person who can configure settings properly accordingly to their environment. It also requires the person to understand the report generated by the tool and makes some sense of it.


Planning
Working with a customer to clearly define and document assessment objectives, scope, and rules of engagement.
1
2
Gathering Information
Collecting and examining key information about an application and its infrastructure.
Security Testing Methodology
Discovering Vulnerabilities
Finding existing vulnerabilities, using both manual and automated techniques.
3
4
Reporting
Providing a comprehensive report with deep analysis and recommendations on how to mitigate the discovered vulnerabilities.

Manual Approach to VAPT

The manual approach depends purely on the ability of the tester. From one to another the skills may vary. This approach is the most common practice in the industry, as it brings out more of the business logic vulnerabilities rather than generic vulnerabilities which automated tools can also produce. This approach is time-consuming and costly, however, it is the most beneficial to an organization in finding business logic vulnerabilities were any automated tool cannot compete with.

In some high-security environments, where the consultant's system may not be connected on the production network; Consultants may be provided with a system with a fresh copy of a pen-testing OS or you have limited tools to work it and not even automated tools. In such cases, it boils down to the capability of the tester and the years of experience a person has. However, false positives are not a concern in this approach as they are validated before giving in the report. Advantages to this approach are reliability and are focused on the scope of concern. Also, it can be stopped at any time, the tester is given clear and concise instructions to what extent the exercise shall be conducted. Example: a manual pen test can be stopped at any given moment or to what extent the tester can go; if a payload is getting blocked a tester can try encoding it differently in which case, the endpoint may probably fail to recognize and block the payload resulting in the command being executed successfully. Similarly, zero-day vulnerabilities can be discovered using this approach which is absolutely critical.

Downfalls; an inexperienced tester could miss out on vulnerabilities given to the client and later if the client gets hacked or has performed this exercise from another vendor and they give more result than the previous vendor, it might deteriorate a firm's brand and more importantly, it would give the client a false sense of security. Here the tester can test as per his knowledge which is to an extent and miss out on things. This approach is time-consuming and not all assessments need to be done manually.

Best of Both Worlds

However, all assessments cannot rely on the automated approach or the manual approach exclusively. For example, each discovered vulnerability cannot be verified manually whether the patch or update is missing… this is an impossible task and also time-consuming. Hence automated tools came in place which discovers vulnerabilities and later is manually verified to find if any false positives were found in them.

Both have their pros and cons but realistically combining both approaches produce the best results: a result from an automated tool and a skill of the pen tester to identify the vulnerability to validate or exploit further carefully is the way. The automatic approach will cover most to all the well-known vulnerabilities in a short period than a tester can do manually, meanwhile, the tester can focus on the business logic vulnerabilities and later verify the vulnerabilities given by the automated tool. This approach saves both time and money for engagements and produces reliable results.

Recommendation for a company newly doing a VAPT must hire an external firm to assess their environment or systems, these firms will give an accurate report about the security posture of your company. and where the data is critical, having an internal team can be in place for frequent assessments so no new if so, as quickly as possible before any harm can befall. Whereas for the smaller business that doesn’t have enough budget to spend on security can hire external firm once a while and harden their network and systems from any threats lurking. Another important aspect is that the manual pen testers need to upgrade their skill sets regularly and get security training periodically.

Having said that, in the end, if an organization needs to get compliant as per a regulatory standard then deciding which approach to use or having an internal team within an organization with the required tools is not applicable. As all regulatory standards mandates organizations to get assessed through a third-party assessor, an external pen testing firm, both the automated and manual approach to give the organization the effective output from the engagements.

REFERENCES

- https://www.vistainfosec.com/blog/automated-vs-manual-approach-to-vulnerability-assessment-penetration-testing-vapt/
- https://www.fortinet.com/resources/cyberglossary/firewall-as-a-service-fwaas#:~:text=FWaaS%20is%20a%20firewall%20solution,Name%20System%20(DNS)%20security.
- https://www.cloudflare.com/learning/cloud/what-is-a-cloud-firewall/
- https://www.intruder.io/automated-penetration-testing
- https://www.indusface.com/