ASSIGNMENT- 18

1)

Explain the different types of firewalls. Discuss the policies and rules of any firewalls. What are the benefits derived? Discuss the best practices for the firewall configurations.

ANS:-

Firewalls monitor traffic against a set of predetermined rules that are designed to sift out harmful content. While no security product can perfectly predict the intent of all content, advances in security technology make it possible to apply known patterns in network data that have signaled previous attacks on other enterprises.

Five types of firewall include the following:

1. *packet filtering firewall*
2. *circuit-level gateway*
3. *application-level gateway (aka proxy firewall)*
4. *stateful inspection firewall*
5. *next-generation firewall (NGFW)*

Firewall devices and services can offer protection beyond standard firewall function -- for example, by providing an intrusion detection or prevention system (IDS/IPS), denial-of-service (DoS) attack protection, session monitoring, and other security services to protect servers and other devices within the private network. While some types of firewalls can work as multifunctional security devices, they need to be part of a multilayered architecture that executes effective enterprise security policies.

1. Packet filtering firewall

Packet filtering firewalls operate inline at junction points where devices such as routers and switches do their work. However, these firewalls don't route packets; rather they compare each packet received to a set of established criteria, such as the allowed IP addresses, packet type, port number and other aspects of the packet

protocol headers. Packets that are flagged as troublesome are, generally speaking, unceremoniously dropped -- that is, they are not forwarded and, thus, cease to exist.

Packet filtering firewall advantages

- *A single device can filter traffic for the entire network*
- *Extremely fast and efficient in scanning traffic*
- *Inexpensive*
- *Minimal effect on other resources, network performance and end-user experience*

Packet filtering firewall disadvantages

- *Because traffic filtering is based entirely on IP address or port information, packet filtering lacks broader context that informs other types of firewalls*
- *Doesn't check the payload and can be easily spoofed*
- *Not an ideal option for every network*
- *Access control lists can be difficult to set up and manage*

Packet filtering may not provide the level of security necessary for every use case, but there are situations in which this low-cost firewall is a solid option. For small or budget-constrained organizations, packet filtering provides a basic level of security that can provide protection against known threats. Larger enterprises can also use packet filtering as part of a layered defense to screen potentially harmful traffic between internal departments.

2. Circuit-level gateway

Using another relatively quick way to identify malicious content, circuit-level gateways monitor TCP handshakes and other network protocol session initiation messages across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimate -- whether the

remote system is considered trusted. They don't inspect the packets themselves, however.

Circuit-level gateway advantages

- *Only processes requested transactions; all other traffic is rejected*
- *Easy to set up and manage*
- *Low cost and minimal impact on end-user experience*

Circuit-level gateway disadvantages

- *If they aren't used in conjunction with other security technology, circuit-level gateways offer no protection against data leakage from devices within the firewall*
- *No application layer monitoring*
- *Requires ongoing updates to keep rules current*

3. Application-level gateway

This kind of device -- technically a proxy and sometimes referred to as a proxy firewall -- functions as the only entry point to and exit point from the network. Application-level gateways filter packets not only according to the service for which they are intended -- as specified by the destination port -- but also by other characteristics, such as the HTTP request string.

While gateways that filter at the application layer provide considerable data security, they can dramatically affect network performance and can be challenging to manage.

Application-level gateway advantages

- *Examines all communications between outside sources and devices behind the firewall, checking not just address, port and TCP header information, but the content itself before it lets any traffic pass through the proxy*

- *Provides fine-grained security controls that can, for example, allow access to a website but restrict which pages on that site the user can open*
- *Protects user anonymity*

Application-level gateway disadvantages

- *Can inhibit network performance*
- *Costlier than some other firewall options*
- *Requires a high degree of effort to derive the maximum benefit from the gateway*
- *Doesn't work with all network protocols*

Application-layer firewalls are best used to protect enterprise resources from web application threats. They can both block access to harmful sites and prevent sensitive information from being leaked from within the firewall. They can, however, introduce a delay in communications.

4. Stateful inspection firewall

State-aware devices not only examine each packet, but also keep track of whether or not that packet is part of an established TCP or other network session. This offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.

A further variant of stateful inspection is the multilayer inspection firewall, which considers the flow of transactions in process across multiple protocol layers of the seven-layer Open Systems Interconnection (OSI) model.

Stateful inspection firewall advantages

- *Monitors the entire session for the state of the connection, while also checking IP addresses and payloads for more thorough security*
- *Offers a high degree of control over what content is let in or out of the network*

- *Does not need to open numerous ports to allow traffic in or out*
- *Delivers substantive logging capabilities*

Stateful inspection firewall disadvantages

- *Resource-intensive and interferes with the speed of network communications*
- *More expensive than other firewall options*
- *Doesn't provide authentication capabilities to validate traffic sources aren't spoofed*

Most organizations benefit from the use of a stateful inspection firewall. These devices serve as a more thorough gateway between computers and other assets within the firewall and resources beyond the enterprise. They also can be highly effective in defending network devices against particular attacks, such as DoS.

5. Next-generation firewall

A typical NGFW combines packet inspection with stateful inspection and also includes some variety of deep packet inspection (DPI), as well as other network security systems, such as an IDS/IPS, malware filtering and antivirus.

While packet inspection in traditional firewalls looks exclusively at the protocol header of the packet, DPI looks at the actual data the packet is carrying. A DPI firewall tracks the progress of a web browsing session and can notice whether a packet payload, when assembled with other packets in an HTTP server reply, constitutes a legitimate HTML-formatted response.

NGFW advantages

- *Combines DPI with malware filtering and other controls to provide an optimal level of filtering*
- *Tracks all traffic from Layer 2 to the application layer for more accurate insights than other methods*

- *Can be automatically updated to provide current context*

NGFW disadvantages

- *In order to derive the biggest benefit, organizations need to integrate NGFWs with other security systems, which can be a complex process*
- *Costlier than other firewall types*

NGFWs are an essential safeguard for organizations in heavily regulated industries, such as healthcare or finance. These firewalls deliver multifunctional capability, which appeals to those with a strong grasp on just how virulent the threat environment is. NGFWs work best when integrated with other security systems, which, in many cases, requires a high degree of expertise.

2. Discuss the configuration and rule sets for ModSecurity. Explain briefly the features and functionalities of the Imperva SecureSphere WAF.

ANS:-

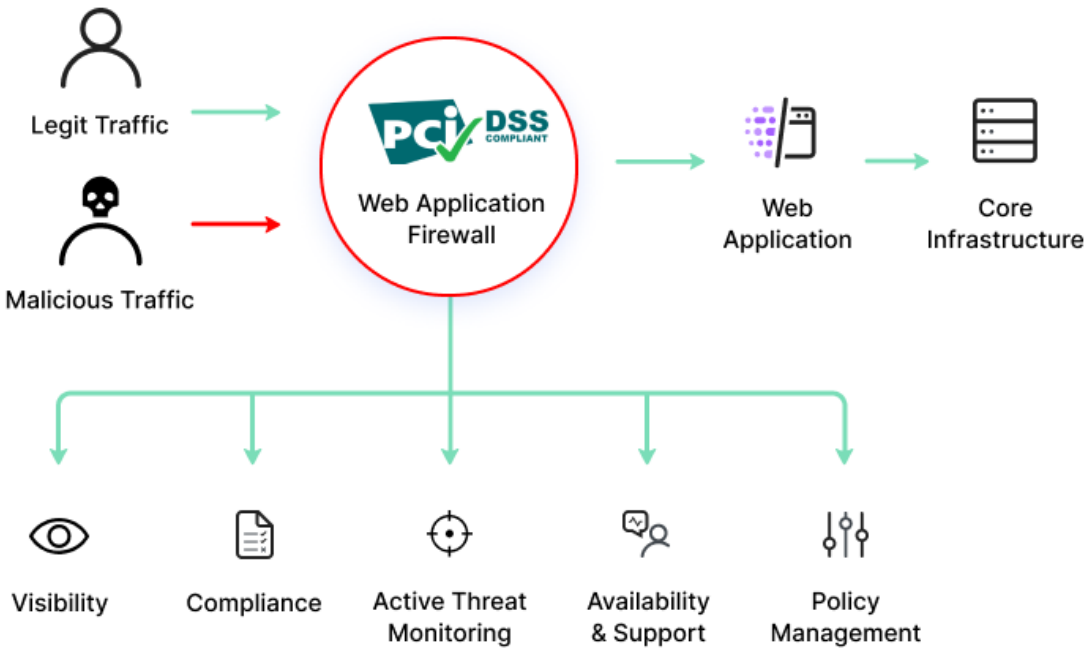
A web application firewall, or WAF, is a security tool for monitoring, filtering and blocking incoming and outgoing data packets from a web application or website. WAFs can be host-based, network-based or cloud-based and are typically deployed through reverse proxies and placed in front of an application or website (or multiple apps and sites).

WAFs are important for a growing number of organizations that offer products or services online—this includes mobile app developers, social media providers, and digital bankers. A WAF can help you protect sensitive data, such as customer records and payment card data, and prevent leakage.

Organizations usually store much of their sensitive data in a backend database that can be accessed through web applications. Companies are increasingly employing mobile applications and IoT devices to facilitate business interactions, with many online transactions occurring at the application layer. Attackers often target applications to reach this data.

Using a WAF can help you meet compliance requirements such as PCI DSS (the Payment Card Industry Data Security Standard), which applies to any organization handling cardholder data and requires the installation of a firewall. A WAF is thus an essential component of an organization's security model.

It is important to have a WAF, but it is recommended you combine it with other security measures, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and traditional firewalls, to achieve a defense-in-depth security model.



WAF workflow

Types of Web Application Firewalls

There are three primary ways to implement a WAF:

- ***Network-based WAF**—usually hardware-based, it is installed locally to minimize latency. However, this is the most expensive type of WAF and necessitates storing and maintaining physical equipment.*

- ***Host-based WAF****—can be fully integrated into the software of an application. This option is cheaper than network-based WAFs and is more customizable, but it consumes extensive local server resources, is complex to implement, and can be expensive to maintain. The machine used to run a host-based WAF often needs to be hardened and customized, which can take time and be costly.*
- ***Cloud-based WAF****—an affordable, easily implemented solution, which typically does not require an upfront investment, with users paying a monthly or annual security-as-a-service subscription. A cloud-based WAF can be regularly updated at no extra cost, and without any effort on the part of the user. However, since you rely on a third party to manage your WAF, it is important to ensure cloud-based WAFs have sufficient customization options to match your organization's business rules.*

WAF Features and Capabilities

Web application firewalls typically offer the following features and capabilities:

	***Attack signature databases***	*Attack signatures are patterns that may indicate malicious traffic, including request types, anomalous server responses, and known malicious IP addresses. WAFs used to rely predominantly on attack pattern databases that were less effective against new or unknown attacks.*
	***AI-powered traffic pattern analysis***	*Artificial intelligence algorithms enable behavioral analysis of traffic patterns, using behavioral baselines for various types of traffic to detect anomalies that indicate an attack. This allows you to detect attacks that don't match known malicious patterns.*

Application profiling

This involves analyzing the structure of an application, including the typical requests, URLs, values, and permitted data types. This allows the WAF to identify and block potentially malicious requests.

Customization

Operators can define the security rules applied to application traffic. This allows organizations to customize WAF behavior according to their needs and prevent the blocking of legitimate traffic.

Correlation engines

These analyze incoming traffic and triage it with known attack signatures, application profiling, AI analysis, and custom rules to determine whether it should be blocked.

DDoS protection platforms

You can integrate a cloud-based platform that protects against distributed denial of service (DDoS) attacks. If the WAF detects a DDoS attack, it can transfer the traffic to the DDoS protection platform, which can handle a large volume of attacks.

	***Content delivery networks (CDNs)***	*WAFs are deployed at the network edge, so a cloud-hosted WAF can provide a CDN to cache the website and improve its load time. The WAF deploys the CDN on several points of presence (PoPs) that are distributed globally, so users are served from the closest PoP.*

WAF Technology

A WAF can be built into server-side software plugins or hardware appliances, or they can be offered as a service to filter traffic. WAFs can protect web apps from malicious or compromised endpoints and function as reverse proxies (as opposed to a proxy server, which protects users from malicious websites).

WAFs ensure security by intercepting and examining every HTTP request. Illegitimate traffic can be tested using a variety of techniques, such as device fingerprinting, input device analysis, and CAPTCHA challenges, and if they appear not to be legitimate, they can be blocked.

WAFs are pre-loaded with security rules that can detect and block many known attack patterns – these typically include the top web app security vulnerabilities maintained by the Open Web Application Security Project (OWASP).

In addition, the organization can define custom rules and security policies to match their application business logic. It can require special expertise to configure and customize a WAF.

WAF Security Models

WAFs can use a positive or negative security model, or a combination of the two:

- ***Positive security model**—the positive WAF security model involves a whitelist that filters traffic according to a list of permitted elements and actions—anything not*

on the list is blocked. The advantage of this model is that it can block new or unknown attacks that the developer didn't anticipate.

- ***Negative security model****—the negative model involves a blacklist (or denylist) that only blocks specific items—anything not on the list is allowed. This model is easier to implement but it cannot guarantee that all threats are addressed. It also requires maintaining a potentially long list of malicious signatures. The level of security depends on the number of restrictions implemented.*

3. Discuss the features of the Barracuda Web Application Firewall (BWAF). Explain the use-case example of this firewall, including scenarios, challenges, solutions, and benefits.

ANS:-

Barracuda Web Application Firewall protects applications, APIs, and mobile app backends against a variety of attacks including the OWASP Top 10, zero-day threats, data leakage, and application-layer denial of service (DoS) attacks. By combining signature-based policies and positive security with robust anomaly-detection capabilities, Barracuda Web Application Firewall can defeat today's most sophisticated attacks targeting your web applications.

Barracuda Active DDoS Prevention — an add-on service for the Barracuda Web Application Firewall — filters out volumetric DDoS attacks before they ever reach your network and harm your apps. It also protects against sophisticated application DDoS attacks without the administrative and resource overhead of traditional solutions, to eliminate service outages while keeping costs manageable for organizations of all sizes.

Stop bad bots dead in their tracks.

Sophisticated malicious bots mimic human users to evade standard bot detection. However, blocking legitimate bots can harm your business. So modern bot defense has to both distinguish between legitimate and malicious bots, and between human users and advanced bots. Barracuda Web Application Firewall offers Advanced Bot Protection that uses machine learning to continually improve its ability to spot and block bad bots and human-mimicking bots — while allowing legitimate human and bot traffic to proceed with minimal impact.

Protect our APIs and mobile apps.

Modern applications are increasingly interconnected, exposing more APIs to attacks. Barracuda Web Application Firewall solutions protect your entire attack surface, including REST APIs and API-based applications. XML protection secures REST and WSDL interfaces against schema and WSDL poisoning. JSON protection scans payloads to ensure that only legitimate requests are allowed through. API Discovery features use your API definition files to automatically create the required rulesets for the API, reducing admin overhead.

Enable granular access control and secure app delivery.

To ensure that only authorized personnel can access your application backends and data, Barracuda Web Application Firewall solutions integrate with AD, LDAP, and RADIUS, giving you granular control over which users and groups can access what data. They also secure all the services that rely on ADFS. SAML support provides a seamless single-sign-on (SSO) experience across your on-premises and cloud-hosted applications. Two-factor authentication further enhances security through integrations with RSA SecureID, SMS PASSCODE, Duo, and others.

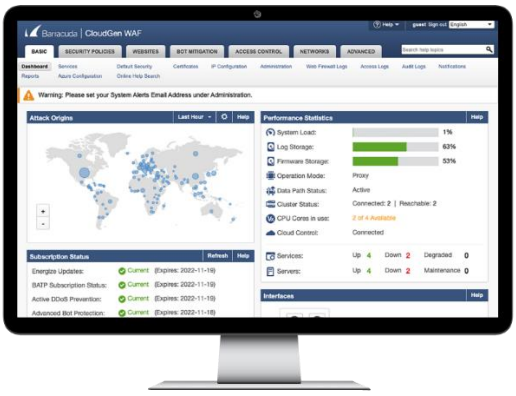
Barracuda Web Application Firewall features a hardened SSL/TLS stack that provides a secure HTTPS front end to your applications. With pre-built templates, you can immediately set up secure TLS ciphers and protocols for standards compliance with ease.

The built-in application delivery module enables HTTP load balancing, content routing, caching, and compression. The content routing module can be used to direct traffic to various applications based on the characteristics of incoming traffic — for instance, a different server for a PC versus mobile client. Connection pooling, caching, and compression capabilities speed traffic delivery and improve user experience by reducing server load and reducing latency.

Automate and orchestrate security.

Barracuda Web Application Firewall integrates with many popular third-party DevOps tools to ensure CI/CD processes are fully automated. Full-featured REST API seamlessly integrates with Puppet, Chef, Ansible, Terraform, Azure ARM, AWS CloudFormation, and more. In addition, the content routing module further enables CI/CD rollout options such as blue-green deployments, canary rollouts and A/B testing. The Barracuda Web Application Firewall's REST API is built on OpenAPI specifications, making it easy to create automation scripts, and the official GitHub page has code samples for popular platforms and use cases.

Barracuda Web Application Firewall solutions leverage Barracuda Vulnerability Manager and Remediation Service to let you remediate app vulnerabilities with a single click and deploy new and updated apps with full confidence. Barracuda Web Application Firewall also supports many third-party vulnerability scanning tools such as IBM AppScan, Rapid7, Immuniweb, HPE Security WebInspect, and more to give you complete freedom and control over vulnerability mitigation.



Gain deep visibility into attacks and traffic patterns.

Barracuda Web Application Firewall features a detailed dashboard that presents vast amounts of data in the form of actionable insights that help you make informed decisions. System health and utilization, traffic patterns, subscription status, system performance, attack statistics and origin locations, and much more is layered into a streamlined dashboard that makes it all easy to interpret and use. Barracuda Web Application Firewall also supports many external SIEMs and log management tools such as Azure Sentinel, Loggly, Sumologic, HPE ARCsight, IBM QRadar, Splunk, and many more.