Exp - 11

* Title: Implement functionality of Firewall using packet filtering and application layer filtering.

* Objective: To understand the functionality of firewall through the implementation of packet filtering and application layer filtering techniques.

* Mode used: Cisco Packet Tracer

* Theory: 1) Packet Filtering: Packet filtering is a firewall technique that examines packets of data as they pass through the firewall and make decisions to allow or deny their transmission based on predefined rules. These rules can be based on various criteria such as source/destination IP addresses, port numbers, protocol types, etc.

2) Application Layer Filtering: Application layer filtering operates at a higher level of the OSI model compared to packet filtering. It inspects the actual contents of the data packets to make decisions about whether to allow or block them. This technique is more sophisticated and can provide granular control over specific applications or protocols.

* Procedure: 1) Setup Network Topology.
2) Configure Firewall Devices: * Access the configuration interface of the firewall devices.
* Define interface connected to internal and external networks.
* Set up IP addresses and subnet mask.
3) Configure Application Layer Filtering: * Implement application layer filtering rules to control access to specific applications or protocols.
* Define policies to inspect the contents of data packets and make decisions based on application-layer formation.
4) Implement Packet Filtering Rules: * Define packet filtering rules such as — Source and destination IP, source and destination port numbers.
* Configure access control lists to permit or deny traffic based on these rules.
5) Test Firewall Configuration: * Generate network traffic from internal hosts to external destinations and vice-versa.
* Monitor traffic flow through firewall devices.

* Observations: Packet filtering effectively controlled traffic based on predefined criterias, ensuring authorized access and preventing unauthorized intrusion. Application Layer Filtering offered granular control over specific protocols.

* Conclusion: Successfully implemented the functionality of a firewall using packet filtering and application layer filtering techniques. We learned how firewalls can be configured to control the flow of network traffic and provide security by enforcing rules and policies at both the packet and application layers. This is important for designing and managing secure network infrastructures in real-world scenarios.

* Questions: 1] What is the fundamental principle behind Packet Filtering in firewall configurations?

Ans: Fundamental principle is to selectively permit or deny network traffic based on predefined rules and criteria. This process involves inspecting individual packets of data as they pass through the firewall and making decisions about whether to allow or block their transmission.

2] How does Packet Filtering differ from other firewall techniques?

Ans: *Packet filtering differs from other firewall techniques primarily in the level at which it operates and the criteria it uses to make decisions about network traffic.

* Packet filtering operates at network layer of OSI model, whereas other techniques operate at higher layers of OSI model.

* Packet filtering makes decisions based on information contained in packet headers, such as sour e and

destination IP addresses, port numbers. Other techniques may consider additional factors such as stateful inspection.
* Packet filtering imposes minimal overhead, whereas other techniques may introduce more processing overhead.

3] What are some criteria commonly used in Packet Filtering rules?
Ans: * Source IP address - It allows administrators to control traffic originating from specific hosts, networks, or IP ranges.
* Destination IP address - It enables administrators to restrict traffic originating from specific hosts.
* Source Port Number - It allows administrators to control traffic from specific application services or protocols running on source host.
* Destination Port Number - It enables administrators to restrict traffic originating from specific application.
* Protocol Type - It allows administrators to selectively permit or deny traffic based on underlying network protocol used.

4] What are advantages and limitations of Packet Filtering as a firewall technique?
Ans: * Advantages : 1) Simplicity - It is relatively simple to implement and manage. It operates at network layer of OSI model and examines packet headers, making it a straight forward

method for controlling traffic.
2) Low Overhead - It imposes minimal overhead because it examines packet headers rather than inspecting contents of each packet.
3) Fast Processing - It can be performed quickly since it operates at a low-level and evaluates packets based on predefined rules.
4) Scalability - It can scale effectively to handle large volumes of network traffic.

* Limitations: 1) Limited Granularity - It provides limited granularity for controlling traffic.
2) Lack of context - It lacks contextual awareness, meaning it cannot make decisions based on context of network connections.
3) Vulnerable to IP spoofing - It is vulnerable to IP spoofing attacks, where attacker forges source IP address of packets to bypass filtering rules.

5] How does Application Layer Filtering complement Packet Filtering in enhancing network security?
Ans: * Provides deep packet inspection beyond header analysis.
* Enabling content-based filtering to block specific keywords or file types.
* Recognising higher-layer protocols for targeted protection against application layer attacks.
* Offering granular access control over individual applications.

* Detecting advanced threats like malware propagation through encrypted channels.