Types of firewalls

1)Packet filter

2)Stateful Inspection Firewall

3)Application Proxy

4)Guard

5)Personal firewall

Think about network communication, what can it contain

On a basic level, looking at things like TCP packets.

1)Packet filter

Packet will always have source address. Packet will always have destination address.

Will have Port number

In headers of packets ,there is port number.

Ports are standard places where your computer and computer you are speaking to speak the same protocol.

Ports are virtual points where network connections start and end. They are used in the transport layer of the Internet protocol suite to differentiate multiple endpoints on a single network interface.

When a computer communicates over a network, it uses a specific port number to identify the type of service or protocol it is using. For example, when you browse the web, your browser typically uses port 80 for HTTP (Hypertext Transfer Protocol) or port 443 for HTTPS (HTTP Secure). This allows your computer to communicate with the web server hosting the website you're visiting

Similarly, other services like email (SMTP, IMAP), FTP (File Transfer Protocol), and SSH (Secure Shell) use other designated ports. This system ensures that when data packets arrive at a computer, the operating system knows which application or service they are intended for, based on the port number they're tagged with.

HTTP – port 80Top of Form

For sending emails ,use SMTP protocol

Connect to terminals over network -> use SSH protocol.

The SSH protocol, or Secure Shell, is a network protocol that provides a secure way to access a remote computer. It is commonly used by network administrators to control web and other types of servers remotely.

Firewall is access control for network communications. Firewall configured with something like an access control matrix.

Might want to limit access to certain protocols from and to my machine

If only surfing web, might only want port 80 active.

When speaking to network outside home environment, should be firewall there between home and outside environment.

Firewall accept packet from inside going out or outside coming in ,check source addresse,dest address,port if it is according to access control security policy ,if okay pass it on else drop it.

Packet filter is in Network(internet) layer.

Application

Transport

Network(Internet ) Layer

Data link( Interface)

Physical Layer

See there are packets but don’t know what they are about at this level ,do know where they are coming from and where they are going ,that’s what packet filter can look at.

2)Stateful inspection firewall

it's a type of firewall that foils any illicit connection attempts from a foreign source, as well as analyzes the contents of the captured packet to discern any false patterns in it.

A stateful inspection firewall is a sophisticated type of firewall that not only monitors the state and context of network traffic, but also inspects the contents of individual packets. This technology enhances security by:

1. **Monitoring Connections:** It keeps track of active connections and understands the state of network traffic (e.g., whether a packet is part of an existing conversation or a new connection attempt). This allows the firewall to make more informed decisions about which packets to allow or block.
2. **Inspecting Packet Contents:** Beyond just examining header information (like source and destination addresses), a stateful inspection firewall delves into the payload of the packet. This enables it to detect and block potentially harmful content, such as malware or specific attack signatures.
3. **Blocking Illicit Attempts:** By analyzing both the state of the connection and the contents of packets, the firewall can effectively identify and block unauthorized access attempts from external sources. This includes preventing various types of network attacks that might exploit vulnerabilities in open connections.
4. **Dynamic Filtering:** The firewall dynamically adjusts its filtering rules based on the ongoing analysis of traffic patterns. This adaptability makes it more effective against sophisticated and evolving cyber threats.

In essence, a stateful inspection firewall offers a more advanced and thorough approach to network security compared to traditional, stateless firewalls, which only look at individual packets in isolation without considering the state of network connections.

There are games which can be played by attacker to get past packet filter.

Payload – stuff we are communicating.

Might be nasty on application level.

If using packet filter attacker can chop packet into smaller pieces. You will never get the full pattern and you will never be able to recognise it is nasty. Putting things together necessary to check if they are nasty or not.

Imagine transmitting things to another party. Would like to block pings. If anyone from outside pinging machine. Someone should never know if my machine awake or not.

Someone can send me a reply to a message I never sent.

If I send a message other party can find out

Firewall – host that mediates access to a network , allowing or disallowing certain types of access on the basis of configured security policy.

Systems that sit between an organization’s internal network and some external network such as internet.

Controls access between the networks. A firewall can filter network traffic before it reaches target host.

Can also redirect network connections as appropriate, or throttle traffic to limit traffic flowing into or out of network.

2 basic types of firewalls

1)First accepts or rejects messages based on basis of packet header information, like destination addresses or ports.

A filtering firewall performs access control on basis of attributes of packet headers, like destination addresses, source addresses and options.

Routers ,other infrastructure -example of filtering firewalls

Allow connections through the firewall

2)Second type of firewall never allows direct connection. Agents called proxies control flow of information through firewall.

Proxy -> intermediate agent or server that acts on behalf of endpoint without allowing direct connection between the 2 endpoints.

3)Application Proxy

Moving up in levels and realizing there can be things wrong with certain applications. Seen how HTTP could be a problem. HTTP can contain not only HTML but also contains things like malicious JavaScript.

Can stop those in browser by configuring browser.

Maybe I would like to stop those before they get into the home network. In case one of my children has misconfigured network or browsers in network.

There might be attack on things at application level.

Proxy firewall (Application level firewall ) uses proxies to perform access control.

A proxy firewall adds to filtering firewall ability to base access on content, either at packet level or higher level of abstraction.

A proxy can base access control on contents of packets and messages ,as well as attributes of packet headers.

Stateful firewall – firewall that keeps track of state of each connection.

Organizations typically partition network into several parts with firewalls between parts to prevent information from leaking.

Common arrangement -> have 2 different internal networks ,one accessible to public and other not.

DMZ – portion of a network that separates a purely internal network from external network.

When information moves from Internet to internal network, confidentiality is not an issue.

There are firewalls between internet and DMZ and between DMZ and internal network.

When information moves from internet to internal network, integrity is issue.

When information moves from internal network to internet ,confidentiality and integrity is an issue.

A screenshot of a computer

Description automatically generated

The principal objective of a stateful firewall's existence is essentially to deter and even drop packets originating from a foreign source, recoding details about them.

This leads us to infer that options A and D can't be a suitable phenomenon.

About option B, when you trigger an XSS attack, being a non-network-based attack, the firewall wouldn't detect it, and would go untraced, posing peril to the system.

I haven't really heard about the attack mentioned in option C, but I'll attempt making an explanation of my version about it. Perhaps, when you send out an encrypted VPN connection to an external site, there isn't sufficient data to discern the illegitimacy of the incoming packet and the firewall would surmise the connection to be a legitimate one, owing to the presence of encrypted pieces of information in the captured packet, which might be in the guise of a valid one. Henceforth, this phenomenon could pose serious imminent hazard to the system.

XSS attack

An XSS (Cross-Site Scripting) attack is a type of security vulnerability typically found in web applications. It allows attackers to inject malicious scripts into web pages viewed by other users. The attack occurs when an application includes untrusted data in a web page without proper validation or escaping, allowing attackers to execute scripts in the victim's browser, which can hijack user sessions, deface websites, or redirect the user to malicious sites.

Here's an overview of how XSS attacks work and their types:

**How XSS Attacks Work:**

1. **Injection of Malicious Script**: The attacker finds a way to insert a malicious script (usually JavaScript) into a webpage.
2. **Script Execution in User's Browser**: When other users visit the compromised page, the malicious script executes in their browsers.
3. **Malicious Actions**: The script can perform actions on behalf of the users, access sensitive data, steal cookies/session tokens, or even rewrite the content of the webpage.

**Types of XSS Attacks:**

1. **Stored XSS (Persistent XSS)**:
   * The malicious script is permanently stored on the target server (e.g., in a database, message forum, visitor log, or comment field).
   * The user retrieves the malicious script from the server when they access the affected page.
2. **Reflected XSS (Non-Persistent XSS)**:
   * The malicious script is reflected off a web server, such as in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request.
   * Typically delivered via a link, which leads to the execution of the script when clicked.
3. **DOM-based XSS**:
   * The vulnerability is in the client-side code rather than the server-side code.
   * The attack occurs when the web application's client-side script writes data provided by the user to the Document Object Model (DOM) without proper sanitization.
4. **Packet Filtering Firewall**:
   * **Function**: Operates at the network level and examines headers of packets to determine whether to allow or block them based on predefined rules (like IP addresses, port number, protocol).
   * **Use**: Commonly used in routers and as a first line of defense due to its simplicity and low resource consumption.
5. **Stateful Inspection Firewall**:
   * **Function**: Monitors the state and context of network traffic (not just individual packets). Inspects both the headers and the payload of packets, maintaining a table of active connections.

State -(e.g., whether a packet is part of an existing conversation or a new connection attempt)

* + **Use**: Provides a more sophisticated level of protection than packet filtering firewalls by understanding and tracking the state of network connections.

1. **Application Proxy Firewall** (or Application-Level Gateway):
   * **Function**: Acts as an intermediary (proxy) between users and the services they access. Examines traffic at the application layer to ensure that only valid data for a particular application is passed.
   * **Use**: Common in securing web applications, where it can scrutinize the content of web traffic to prevent attacks like SQL injection or cross-site scripting.
2. **Guard**:
   * **Function and Use**: This term is less standard in the field of firewalls. It might refer to a specific brand or product, or it could be a generic term for a firewall with specialized or advanced features. Without specific context, it's challenging to provide a detailed explanation. It's possible that in some contexts, "Guard" could refer to a firewall with advanced security features or a firewall designed for a specific purpose.
3. **Personal Firewall**:
   * **Function**: Software-based firewall designed to protect an individual computer or device from unauthorized access. It controls incoming and outgoing network traffic based on a set of user-defined rules.
   * **Use**: Commonly used in consumer devices like personal computers, laptops, and smartphones. It's a key component in comprehensive endpoint security.

It's important to note that the effectiveness of a firewall depends on how well its rules and policies are configured and maintained. Additionally, firewalls are often used in combination with other security measures to provide layered defense against various types of cyber threats.