Internet Today: A Deep Dive into Firewalls

Presentation Report

By:

NET212

NETWORKING 1

Ms. Kiana Arabela Eslita

INTERNET

There is no denying that the Internet, an influential force that appeared in the second half of the 20th century, has completely changed our world in ways that were unimaginable before. Due to its profound impact, society has never been the same, with our daily lives, jobs, and relationships with others entirely changed. The Internet has a major impact on communication, information access, economy, culture, and many other aspects of our lives.

Positive Effects of Internet includes:

- Access to Information
- Communication and Connectivity
- Economic Opportunities
- Education and E-Learning
- Healthcare Advancements
- Entertainment and Media
- Social and Cultural Impact
- Work Flexibility
- Innovation and Creativity

Negative Effects of Internet includes:

- Internet Addiction
- Misinformation and Disinformation
- Online Harassment and Hate Speech

- Loss of Productivity
- Online Scams and Fraud

Conclusion

These days, the Internet is a transformational force that has profoundly changed our world. It has wide-ranging, profound implications on how we work, study, communicate, and pass our time. It is critical that we take advantage of the Internet's advantages while tackling its drawbacks as we traverse the ever changing digital landscape. Ensuring that the Internet remains a good engine for change in our lives and society requires finding a balance between connectivity and privacy, information availability and judgment, and digital empowerment and well-being.

Given how important the Internet is to us in the modern world, let's discuss one of the security measures that should be put in place for our computers. We must ensure that our computer is completely protected because we frequently use it to explore the internet for a wide range of topics. Join me as we unravel the mystery of firewalls. A system security that protect us to trojans

WHAT IS FIREWALL?

The most important aspect of a system is security. Numerous concepts exist for system security. One of the most important concepts related to system security is the firewall. A Defensor can be used as hardware or software that essentially prevents unwanted communication from entering or leaving a network.

Numerous software programs are available to offer network or system security. Firewall devices are employed in a similar way to offer system security. Most of the time, firewalls are employed to stop unauthorized internet users from accessing private networks linked up to the Internet

Key Features of a firewall:

We must understand what a firewall can and cannot do before learning about how it operates. Many different types of firewalls have common features and capabilities that set them apart from one another. Actually, a firewall needs to be able to do crucial tasks:

- Control and arrange traffic
- Authentication access
- Protect organization assets
- Protect network resources from harmful actions while accessing the internet.
- Assure protected and secure access to your internal assets to outside users
- May increase performance of network systems.

Firewall Policy

A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies. Before a firewall policy is created, some form of risk analysis should be performed to develop a list of the types of traffic needed by the organization and categorize how they must be secured including which types of traffic can traverse a firewall under what circumstances.

Policies Based on IP Addresses and Protocols

Firewall policies should only permit appropriate source and destination IP addresses to be used. Specific recommendations for IP addresses include:

- IP Addresses and Other IP Characteristics
    - ❖ Traffic with invalid source or destination addresses should always be blocked, regardless of the firewall location.
    - ❖ Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic should be blocked at the network perimeter.
    - ❖ Traffic with a private destination address for incoming traffic or source address for outgoing traffic should be blocked at the network perimeter.
    - ❖ Incoming traffic with a destination address of the firewall itself should be blocked unless the firewall is offering services for incoming traffic that require direct connections.
- **IPv6**

- ❖ The firewall should be able to use IPv6 addresses in all filtering rules that use IPv4 addresses.
- ❖ The administrative interface should allow administrators to clone IPv4 rules to IPv6 addresses to make administration easier.

Policies Based on Applications

Most early firewall work involved simply blocking unwanted or suspicious traffic at the network boundary. Inbound application firewalls or application proxies take a different approach: they let traffic destined for a particular server into the network, but capture that traffic in a server that processes it like a port-based firewall. The application-based approach provides an additional layer of security for incoming traffic by validating some of the traffic before it reaches the desired server.

- Is a suitable application firewall available? Or, if appropriate, is a suitable application proxy available?
- Is the server already sufficiently protected by existing firewalls?
- Can the main server remove malicious content as effectively as the application firewall or proxy?
- Is the latency caused by an application proxy acceptable for the application?
- How easy is it to update the filtering rules on the main server and the application firewall or proxy to handle newly developed threats?

Firewall Types

This section of the publication provides an overview of firewall technologies and basic information on the capabilities of several commonly used types. Firewalling is often combined with other technologies most notably routing and many technologies often associated with firewalls are more accurately part of these other technologies.

Packet Filtering

The most basic feature of a firewall is the packet filter. Older firewalls that were only packet filters were essentially routing devices that provided access control functionality for host addresses and communication sessions. These devices, also known as *stateless inspection firewalls*, do not keep track of the state of each flow of traffic that passes through the firewall; this means, for example, that they cannot associate multiple requests within a single session to each other.

In their most basic form, firewalls with packet filters operate at the network layer. This provides network access control based on several pieces of information contained in a packet, including:

- The packet's source IP address—the address of the host from which the packet originated (such as 192.168.1.1)
- The packet's destination address—the address of the host the packet is trying to reach (e.g., 192.168.2.1)

Stateful Inspection

Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. This is accomplished by incorporating greater awareness of the transport layer. As with packet filtering, stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule, but unlike packet filtering, stateful inspection keeps track of each connection in a state table.

Table 2-1 provides an example of a state table.

If a device on the internal network (shown here as 192.168.1.100) attempts to connect to a device outside the firewall (192.0.2.71), the connection attempt is first checked to see if it is permitted by the firewall ruleset. If it is permitted, an entry is added to the state table that indicates a new session is being initiated, as shown in the first entry under “Connection State” in Table 2-1. If 192.0.2.71 and 192.168.1.100 complete the three-way TCP handshake, the connection state will change to “established” and all subsequent traffic matching the entry will be allowed to pass through the firewall.

Table 2-1. State Table Example

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	192.0.2.71	80	Initiated
192.168.1.102	1031	10.12.18.74	80	Established
192.168.1.101	1033	10.66.32.122	25	Established
192.168.1.106	1035	10.231.32.12	79	Established

Application-Proxy Gateways

An application-proxy gateway is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality. These firewalls contain a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other, and never allows a direct connection between them.

Firewalls with application-proxy gateways can also have several disadvantages when compared to packet filtering and stateful inspection. First, because of the “full packet awareness” of application-proxy gateways, the firewall spends much more time reading and interpreting each packet. Because of this, some of these gateways are poorly suited to high-bandwidth or real-time applications—but application proxy gateways rated for high bandwidth are available.

Dedicated Proxy Servers

Dedicated proxy servers differ from application-proxy gateways in that while dedicated proxy servers retain proxy control of traffic, they usually have much more limited firewalling capabilities. They are described in this section because of their close relationship to application-proxy gateway firewalls.

Figure 2-2 shows a sample diagram of a network employing a dedicated HTTP proxy server that has been placed behind another firewall system. The HTTP proxy would handle outbound connections to external web servers and possibly filter for active content. Requests from users first go to the proxy, and the proxy then sends the request

(possibly changed) to the outside web server. The response from that web server then comes back to the proxy, which relays it to the user. Many organizations enable caching of frequently used web pages on the proxy to reduce network traffic and improve response times.

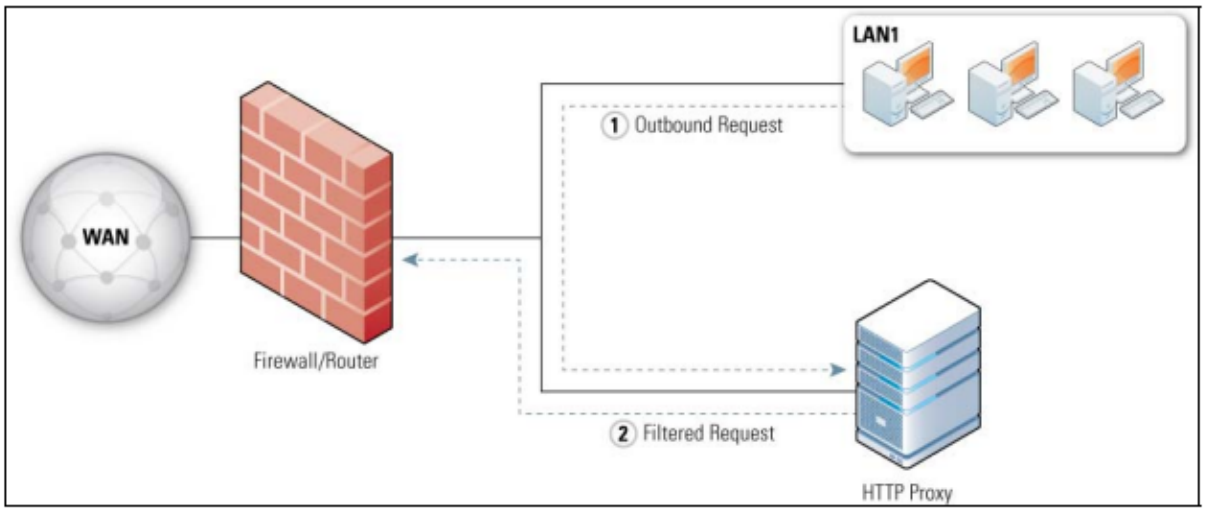

Figure 2-2. Application Proxy Configuration

Pros of firewall | Advantages of firewall:

- A firewall prevents hackers and remote access.
- It protects data.
- Better security and network monitoring features
- It ensures better privacy and security.
- Allow for more advanced network functionality.
- A network-based firewall, such as a router, can protect numerous systems, but an OS-based firewall can only protect single computers.

Cons of firewall | Disadvantages of firewall:

- Depending on the level of sophistication necessary, installing a firewall might be pricey.
- This is harmed because each packet must be authenticated before being let into the network.
- Need for professionals to manage.
- There are a few limitations in a firewall like its inability to prevent virus and malware attacks for which separate applications would be required at the individual system level.
- Firewall maintenance and up-gradation require extra manpower and resources.
- Can slow down your internet speeds.

Conclusion:

Firewalls are becoming a crucial component of a network security policy as the Internet becomes more integrated into business operations. It is crucial for protecting computer systems against external malware attacks such as Trojan horses, spyware, viruses, and other threats. Without affecting the speed of the computer system or network access, a strong firewall offers complete security to our network and system. A few things should always be kept in mind to ensure security: Installing software from unreliable sources is never a good idea. Always download from reputable websites that are accessible online. Prior to using your firewall to monitor any information we wish to send over the internet, be sure it is secure. Installing firewall software on a PC is

essential, as uninfected systems can quickly spread to other PCs linked to the same network.

Firewalls stand as an indispensable shield in our ongoing battle against the ever-evolving landscape of cyber threats. By adhering to fundamental security practices, such as securing our software sources, encrypting our data, and safeguarding every node in our network, we ensure that our digital world remains fortified against external intrusions, allowing us to harness the full potential of the Internet while preserving the integrity and confidentiality of our data.

References:

Pooja , K., & Kaplesh , G. (n.d.). Firewalls: A study on Techniques, Security and Threats. https://www.pramanaresearch.org/gallery/prj-p690.pdf

Scarfone, K., & Hoffman, P. (n.d.). Guidelines on Firewalls and Firewall Policy. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

Bhatnagar, N. (2015, January). A Review on Firewall & Its Advantages and Disadvantages. https://www.researchgate.net/publication/324646511_A_Review_on_Firewall_Its_Advantages_and_Disadvantages

Syed Shah Alam, Nik Mohd. Hazrul Nik Hashim, Maisarah Ahmad, Che Aniza Che Wel, Sallehuddin Mohd Nor, & Nor Asiah Omar. (n.d.). Negative and positive impact of internet addiction on young adults: Empericial study in Malaysia. https://www.redalyc.org/pdf/549/54932488004.pdf