|  |  |
| --- | --- |
| **Application Level Gateway Firewall or Proxy Firewall** | **Packet Filtering Firewall** |
| Examines the content of the data packets and make decisions based on the application-level information contained within them. | It examines individual packets of data as they pass through the firewall, and based on a set of predefined rules, it either allows or blocks the packets.It also only inspects traffic at the network layer (Layer 3) and transport layer (Layer 4) |
| It provides additional security by analyzing and filtering incoming and outgoing traffic based on application-level protocols such as HTTP, FTP, SMTP, and DNS. | Packet filtering firewalls can be used to protect a network from a variety of threats, including denial-of-service attacks, port scanning, and unauthorized access attempts. |
| **Why this firewall?**  Organizations might use an application-level gateway firewall to protect their web servers from attacks such as SQL injection or cross-site scripting (XSS) attacks. The firewall would inspect the incoming HTTP traffic and filter out any malicious requests or data packets that could potentially compromise the web server. | **Why this firewall?**  Its common, and as been around since the first firewalls. Over the years, it has been worked on constantly. Packet filtering is a reliable technique that can provide a high level of security for a network. While it is not foolproof and can be bypassed by sophisticated attackers using techniques such as packet fragmentation or tunneling, it is still a valuable tool in the fight against cyber threats. |
| **Case where it failed**  In 2015, attackers believed to be linked to the Chinese government launched a sophisticated cyber attack on the OPM, which resulted in the theft of sensitive personal information belonging to millions of current and former US government employees. The attack was believed to have been facilitated by a vulnerability in the OPM's application-level gateway firewall, which allowed the attackers to bypass security controls and gain access to the network. | **Case where it failed**  In 2004, a vulnerability was discovered in the Cisco IOS Firewall that allowed attackers to bypass packet filtering rules and gain unauthorized access to the network. In 2011, researchers at the Black Hat security conference demonstrated a technique for bypassing packet filtering firewalls using ICMP packets. |

|  |  |
| --- | --- |
| **Best practices of firewall Implementation and Management** |  |
| Planning routine firewall security audits. | Checking the rules and any policy violations. This should be done, usually when a new firewall is installed or if a lot of configuration is being carried out on the firewall. |
| Making sure the firewall is updated on time | This is to ensure you’re the security of your firewall is upgraded and at its best. This allows the firewall to stay functional and secured, |
| Update the firewall rule base and optimize it. | The rules aka the policies tend to change since things keeps evolving, ensuring the policies doesn’t have any issue in line with the company’s own policies is a very important practice as consequences may arise. Optimizing it is also good as it helps keeping the firewall clean. |