|  |  |
| --- | --- |
| Title | Information |
| **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. |
| **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. |
| **Comparison and contrast of Packet filtering firewalls** | * Packet-filtering firewalls are faster and more efficient than application-level gateway firewalls because they only examine packet headers, not packet contents. * Packet-filtering firewalls are commonly used for basic security needs like protecting against low-level network attacks and filtering out unwanted traffic. * Packet-filtering firewalls are not effective against attacks that exploit application-level vulnerabilities, such as SQL injection and cross-site scripting. |

|  |  |
| --- | --- |
| Title | Information |
| **Comparison and contrast of Packet filtering firewalls** | * Application-level gateway firewalls can examine the contents of packets and apply security policies based on application-specific data, such as HTTP headers and cookies. * They are more secure than packet-filtering firewalls because they can detect and block attacks that exploit application-level vulnerabilities. * Application-level gateway firewalls are commonly used to protect web applications, email servers, and other applications that require granular control over network traffic. * They are slower and more resource-intensive than packet-filtering firewalls because they examine packet contents. |
| **Summary** | * In summary, packet-filtering firewalls are faster and more efficient, but less secure, while application-level gateway firewalls are more secure, but slower and more resource-intensive. * Packet-filtering firewalls are suitable for basic network security needs, while application-level gateway firewalls are more suitable for application security and protection from advanced attacks. |

|  |  |
| --- | --- |
| What are the best practise for firewall implementation and management? | **Harden and Properly Configure the Firewall**   * Most all-in-one firewall solution operating systems are hardened by the vendor. * If you are deploying a software firewall solution, ensure the OS is first patched and hardened.   **Plan your Firewall Deployment**   * Firewalls monitor and control inbound and outbound access across network boundaries in a macro-segmented network. * They can be customized to add more granular control, in a High Availability (HA) cluster or a hyperscale network security solution.   **Secure User Accounts**  Account takeover is a common technique used by cyber threat actors, in order to prevent this, do the following:     * Rename or change default accounts and passwords * Require MFA and/or set a strong password policy (complex passwords with upper and lower case letters, special characters, and numbers, 12 characters or longer, prevent password reuse) * Use role-based access control (RBAC) for firewall admins. Delegate and limit access to match the user’s access need (i.e., allow only read-only access for auditors and create dedicated access roles and accounts for DevSecOps teams)   **Lock Down Zone Access to Approved Traffic**   * Firewalls are used to enforce and monitor access for network segmentation. * In macro-segmentation, the zones are broad groups like external, internal, DMZ, and guest Wi-Fi. In micro-segmentation, the zones may be defined by applications like web apps or databases. * Firewalls control access by setting a firewall policy rule, which broadly defines access based on traffic source and destination. * To detect known bad sites, additional security features can be enabled, such as URL filtering and application control. |
| How to secure a firewall? | **Using Multiple Firewall Solutions at Different Levels**   * No one firewall, no matter how robust, will ever be proof against all attacks. * So, when creating an in depth strategy of defence that segments your network and apps, consider using multiple firewall solutions to protect against multiple vectors of attacks.   **Stay on Top of Security Patches/Updates**   * Many attacks leverage known vulnerabilities in popular software and security tools. * These vulnerabilities frequently have security patches that fix the issue, but many organizations are behind schedule on applying them (which leaves the organization vulnerable). * By applying security patches to your hacker protection software, you can keep cybercriminals out more easily.   **Set Strong Password Policies and Multifactor Authentication**   * Hijacked user accounts are a common tool for attackers to bypass firewall security tools. * So, making it harder to steal and use account credentials can help limit the risk of a breach. * Setting strong password policies (8+ characters long, use case-sensitive letters, adding special characters, etc.) and applying multifactor authentication can help prevent account hijacking.   **Regularly Running Penetration Tests**   * Penetration testing can aid in locating previously undiscovered security vulnerabilities in the applications and services used by your application. * Once discovered, steps can be taken to close these security gaps (hopefully before an attacker can use them). * Some common measures include applying custom patches to software code and firewall rules, or replacing the vulnerable solution with something that is better-protected. |
|  |  |
|  |  |