Part d

Packet filtering

Packet filtering firewalls are one of the earliest and simplest forms of the modern firewall. These types of firewalls are build on the idea of data filtering. When information is send through a connection (via “packet”) the firewall compares each packet to a set of pre-established criteria, usually related to the packet protocol header. IF addresses packet type or port number.

* If the system detects a known attack pattern based on these criteria, it drops the packet and prevents the connection form being made.
* However, the simplicity of the packet filtering firewalls cuts both ways. While these firewalls offer a basic standard of security, they can assess packets only on broad sets of criteria, often related to the service they are being used for or the destination port.
* Compared to the other options, this is a fairly superficial way to prevent malicious traffic, and more advanced security features ( such as intrusion detection) are not typically included.

Circuit level gateway:

* Circuit level gateway are another type of firewall with a slightly different approach. Rather than filtering packets, the gateway crates an intermediate connection between the local and remote hosts.
* This connection offers co-ordination security across the UDP and TCP.
* In essence, the circuit level gateways only allow traffic that can be verified by the web connections TCP handshake. If this verification doesn’t happened, the traffic doesn’t go through.
* Like packet filtering this firewall is simple to understand and deply but it does come with limitations.
* The firewall cant perform deep packet inspections. On the other hand, its simplicity means that it takes few resources to operate and network performance impacts tend to be minimal.

Stateful packet inspections:

* Stateful packet inspections (SPI) firewalls are a but of hybrid combining packet filtering alongside tracking the state of each network session, based on pre established security criteria.
* With stateful inspections firewalls the system monitors both incoming packets and the presence of any TCP connections or any other session level state info to determine how data can be sent. For reference stateful inspections firewalls work within the network layer of the OSI framework.
* And while the scope of OSI model is too big to get into here, business owners can be assured that this firewall method will offer a much higher standard of security than basic packet filtering

Application level gateway ( proxy firewalls)

* Application level gateways are a sophisticated type of firewall that filters traffic at the application layer rather than the circuit level. This is also known as s “proxy firewall” as the system usually involves setting up a proxy server to intercept traffic and validate it against a set of security criteria before sending it through.
* This approach offers great protection against malicious traffic and treat actors, as it combines essential packet detection with session level criteria in a simple hard to penetrate framework.
* Most critically, the application level gateway proxy prevents malicious users from accessing web applications directly. Of course like many sophisticated firewalls the security comes at the expense of system performance.