

**A firewall is essentially a device which historically sits at the border between different networks. So between the public internet, public or private subnets, or maybe the public internet and your business networks. It essentially divides two different networks with different levels of security. The firewall sits between these two and acts as a brick wall it's essentially award that traffic cannot pass unless you allow it.** A firewall is capable of reading the data of packets and either allowing the transit of that packet through it or denying it. So in this case, we've got a firewall. It sits between the public internet and a web server. Different clients can try to access this website, so it might be two different customers, and depending on certain elements of their IP packets, you can decide whether to allow that data through or to deny it and block it and not allow any communication between the client and the server. Now what the firewall can read from this network communication between the client and the server depends on what layer the firewall runs on. So now that you understand the OSI seven layer model, you start to understand the functionality offered by each of these layers.

So if the firewall is a layer three firewall, **so a network layer and all it can do is understand source and destination IP addresses or ranges of IP addresses.** So you might allow one customer based on their IP address or the IP address range that their internet service provider uses and you might deny another customer based purely on their IP address. Maybe they're accessing your website from a Cafe WiFi network that you don't have confidence in, and you could block that by just adding a block rule on the firewall and a layer three firewall can only see source and destination IP addresses or ranges.

Now you might also have a layer four firewall, so a transport layer and this adds the ability to understand the TCP and UDP protocols as well as port numbers. So you might decide to block traffic that's attempting to access the server on anything but port 80. Let's say it's a web server that's just serving traffic out on port 80 then you could block everything else and significantly improve its security.

It might be a layer five firewall so it can understand sessions so you might allow traffic to come from a particular customer as well as allowing all response traffic for that particular session. If it was a layer four or three firewall, you need to allow that traffic in both directions. The initiation and the response if it was layer five it would know that a response from the server to this authorized client if it was a response for this initiation traffic, it would be part the same session. So layer five firewalls have the ability to allow based on sessions, not individual communication streams.

If it's the layer seven firewall then you might be allowing or denying based on application specifics, so you might allow certain clients to connect to certain paths of the application maybe /images or /patient images and disallow certain customers from accessing others. So you might not allow one customer to access the patient imaging of another customer and if it was a layer seven application firewall then potentially, it would be able to understand the HTML paths to make that happen. So this is why it's important to understand for a particular product inside AWS and even wider than AWS know what layer that product operates at because by knowing the layer you'll understand what capabilities it has.

**So if its layer three it's IPs, if it's layer four it's protocols and ports, if it's layer five so like security groups inside AWS then it understands sessions, and you don't need to explicitly think about incoming and outgoing that are part the same session. If it's layer seven you've got a lot of enhanced functionalities that you can start looking in application data and making decisions based on things like malware or SQL injections or other known exploits.** So, ideally, you'd use a layer seven firewall over a layer three or four but be aware that the higher the layer of the firewall, the more compute requirements it comes with. So generally layer seven appliances and layer seven firewalls tend to cost significantly more than firewalls, which operate at lower levels

Essentially, firewalls have a rule base, they analyze incoming or outgoing traffic and the attempt to pattern match based on source and destination IP, source and destination port, application protocol, may be in the case of layer seven firewalls application paths. Each of those pattern matches is called the rule. You allow or deny based on that rule and then the traffic is either allowed through or it's dropped. Keep that in mind when it comes to how you evaluate various different AWS products, such as security groups and network ACLs that we'll talk about in the next topic because both of those are essentially firewalls. One of them operates at layer five and one of them doesn't and now that you know about the OSI seven layer model, you'll start to understand these different capabilities.