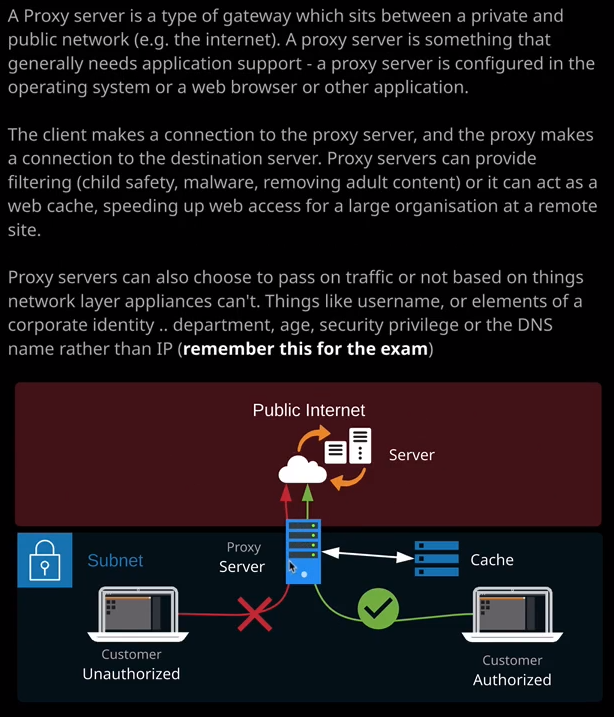
**Proxy Servers**



Now, the architecture of a proxy server is slightly different than a firewall, but it does occupy a similar network location from an architectural point of view. So it sits at the boundary between an internal network and a public network such as the internet but **a proxy server handles outgoing traffic**, where traditionally a firewall handles incoming and outgoing. The use case, though the scenario that you'd use a proxy server is completely different. **A proxy server is a type of gateway, so it sits between the private and public network. So, for example, the internet but a proxy server is something that generally needs application support so you configure a proxy server inside a web browser, an operating system, or another application and what happens is that a client makes a connection to the proxy server, and then the proxy server on its behalf makes a connection to the destination server.**

Now, a common use case or scenario that **proxy servers have is to function as either a caching server**. So you've got lots of different clients that are browsing to the same website then the proxy server can cache common images or large files and then, instead of the remote server delivering these files every single time they're needed, the proxy server can deliver them directly to the client rather than having to use the remote server.   
Proxy servers can also be useful to **perform filtering**, so because these clients are accessing the server indirectly, the proxy server can filter out content that might have child safety concerns. It might contain malware, you might want to remove adult content and obviously, in addition acts is that **web cache so speeding up with accesses** for large organizations or if you've got remote sites, maybe where their internet connections aren't that great. You can put a proxy server in place, and it can speed up access because instead of each individual client having to go out over a slow internet connection to a remote server, you can proxy it inside the network and have the content delivered from that proxy server rather than going out to the public internet. So proxy servers tend to be a type of device that's used on existing on premise physical networks, but knowing about them is really useful for the exam because they do offer a number of extra pieces of functionality.

Inside AWS, you've got a lot of filtering products such as network ACLs or security groups but these filter based on network level factors or, in the case of security groups, it goes up to session but you're not looking at anything above those layers. So AWS filtering products, for example, can't filter things like username in an application or elements of a corporate identity. So department, age, security privileges, or maybe the DNS name of a site rather than the IP. With proxy servers because essentially the clients are making a connection to this proxy server, and then it makes a connection out to the public internet. **This proxy server can perform almost any authentication or validation that it wants.** So if you're running inside a corporate environment and you bring a client device so a laptop onto that network, the proxy server could, in theory, check that you're using a valid corporate ID and if you are, you get relatively unrestricted access. If you're not you might be presented with a guest log in, so there are lots of different ways proxy servers are used but in the exam, **tend to default to proxy server whenever you're looking at something that you know can't be done with AWS products and services**. So if you see a question that talks about filtering based on profile ID or age internal security privilege or applying some sort of filtering based on username, corporate identity, anything like that and one of the answers is to **install a proxy server a proxy application on EC2** then that's potentially a correct answer.

**A proxy server can be installed on an EC2 instance, and it's something that can offer additional functionality over and above what AWS network level filtering can do.** So remember that for the exam you might face one or two questions on that.

So at this point we're going to move on to the AWS private networking topic, and that's where I'm going to introduce a virtual private cloud, or VPC, which is a private networking solution. We can look at subnets inside AWS, routing inside AWS, how network ACLs work, bastion host, lots of other basic AWS networking concepts, so we're going to do that topic next. Then we'll move on to advanced VPC where I'll cover some more advanced networking concepts and then the next two topics after that will be a deep dive into DNS and that's something that's essential to understand both for the exam and production usage. So at this point, that's everything. Go ahead, mark this video as complete, and when you're ready, you can join me in the next topic, which is AWS private networking.