VPNs

Hi. In this video, we're going to look at VPNs, virtual private networks. Very likely that you've come across this term before. In fact, you may have seen adverts on television for a variety of different products offering you these sorts of services.

This video should help you understand a little bit more about how they work. It should be said, that we're not going into significant depth here. So if you are interested, it's worth having a look at the numerous resources which are available on the web. We can generally think of VPNs as having two possible uses.

The first is remote access. This is effectively where you are on a remote site and you wish to appear as if you are within a specific network. For example, if I'm working at home and I want to appear as though I'm working in the University environment, then I can use the university's VPN to achieve this. The other option that you have is site-to-site.

With site-to-site VPN, what we're trying to achieve is that someone who is perhaps at the Glasgow office wants to work with information that's available at the Edinburgh office. So it provides a secure communication channel from one site to another. There are generally three types of VPN.

The first is a trusted VPN. Then we have a secure VPN. And finally, a hybrid VPN. A trusted VPN, we don't tend to see these days. Effectively, these were where companies would have access to their own private lines, which would give them that degree of certainty that that communication was secure, as no one else was able to use those particular lines.

In contrast, a secure VPN uses protocols to ensure secure communication. And as you might imagine, a hybrid VPN is a combination of both. We will focus on a secure VPN. With a secure VPN, it's effectively a combination of three separate mechanisms; tunnelling, authentication, and encryption. Two of these are certainly concepts which should be familiar to you at this point.

We'll address each of these in turn. Let's start off with authentication. When the client makes

a request to the VPN to set up a secure connection, it's asked to authenticate itself. This depends on the protocols which the secured VPN is using. But this could, perhaps, be through a username and password combination or even digital certificates.

Once the VPN is happy that the client has authenticated, it can then move on to set-up, what is referred to as a tunnel. Tunnels can effectively be thought of as packing up your information packets into other packets, obscuring the information that's within. You can think of this as working with an envelope.

Your envelope can have the address of the building on it. So for example, we could send a letter to the 11th floor office of Livingstone Tower. However, within that packet, what we want to do is have some local addressing. So it could then go to my office on the 14th floor. So it would use internal addressing.

It has to get to the building first, using the external facing addressing. And then, from there, it can use the internal addressing. So this masks the local addressing that we might have. It's this process of encapsulating packets within other packets which helps us to mask the structure of the internal network.

But of course, an attacker can still sniff this information, even if we have it layered up in different packets. So our next step is encryption. Packets are encrypted in one of two modes, either transport mode or internal mode. In transport mode, data is encrypted as it's created. However, in tunnel mode, it's encrypted as it is transmitted through the tunnel.

The encryption used obviously varies depending on the secure VPN implementation. So it may be making use of encryption, such as AES. That's a very quick rundown of how VPNs work. I'd like you to take some time now to consider what kind of attacks a VPN might help to mitigate. I hope you've enjoyed the video, and I'll see you next time.