Demilitarized Zones

In this video, we're going to take a look at a couple of approaches for protecting internal networks from external untrusted networks, such as the internet. We'll look at intrusion detection and prevention systems, as well as the demilitarised zone, and how that can be implemented in a firewall approach. A demilitarised zone is part of a network or a complete network placed between the internal network and the external untrusted network, such as the internet.

It's placed to provide an extra layer of segregation from the internal network, and provides extra security since it means that an attacker would have to break past firewalls for each of the layers. It also has the benefit of restricting routes from the private network to the internet and vice versa. This is because the router managing communication to the outside network will only present DMZ in routing table, and DNS exchanges.

Similarly, the router inside the DMZ only presents to the private network. In a demilitarised zone, external-facing server services and resources are located within the subnet of the demilitarised zone. Typically this includes things like web servers. These are accessible from untrusted networks, such as the internet, but the rest of the local area internal network is not. So we can see this in the diagram below, which represents a common 2 firewall architecture for a demilitarised zone. There are two firewalls on either side of the DMZ.

We've got our internal firewall and our perimeter, or externally facing firewall. Anything from our external untrusted network goes through our perimeter firewall first and can access resources, and servers, and services within the demilitarised zone, but the communication stops there for any external network.

The internal firewall will not let anything beyond that point come from the external network. Similarly, on the other side of things, we have the internal network, which can communicate through the internal firewall to the demilitarised zone, but, again, communication cannot go the other way. So you can see an effect. We have the zone in the middle where internal and external can come into it, but cannot go from internal to external or vice versa. Despite having a firewall and potentially a demilitarised zone in place, it's still very likely that your

network will be attacked, so one way of helping with this is by having what's called an intrusion detection system.

This monitors network for unusual behaviour or suspected incidents. An incident is a violation or potential violation of computer security policies, acceptable use policies, or standard security practices. These incidents could result from something such as a denial of service, malware, or unauthorised access. In addition to this, we have something called an Intrusion Prevention System. This is software which has all the capabilities of an Intrusion Detection System, but can also attempt to stop such possible incidents.

So, for example, by blocking access to a particular resource, such as a server, or blocking a particular user IP. The combination of these two technologies can be referred to as an IDPS technology. And these are differentiated primarily by the types of events that we can recognise and the approaches that we use to identify incidents, but all typically perform the following tasks.

First of all, they record information related to observed events often this is information, which is logged locally, and thus could be sent to other systems within an organisation. It also notifies security administrators of important observed events. This is known as an alert. It can be implemented, for example, using emails, or messages on a user interface for the software. An alert typically includes basic information regarding an event with further details upon accessing the UI for the software.

And you can also produce reports which summarise the monitored events or provide details on particular events of interest. So, for example, for use and management, such as redefining or identifying security policies. And it should be noted that IDPS systems can be implemented as part of a firewall. However, as with many things, this is only the first step.

It can't stop a number of different issues, such as administrator misconfiguration, the insider threat, or social engineering. Well, that's us for this video. We've had a look at demilitarised zones, and how they can be applied in terms of a firewall, and we've also had to look at Intrusion Detection and Prevention systems. I hope you've enjoyed the video, and I'll see you next time.