The Zero Trust Projects

So what's the difference between micro-segmentation and VLANs? Well let's imagine a VLAN as one big house, and everyone inside the house can walk around and enter any room they want. All the doors are open for anyone living, or even visiting the house to enter. However, with micro-segmentation, you can't walk freely around the house. Every door is locked unless you have the keys and the authority to enter. Micro-segmentation takes the traditional zone-based VLAN design and further segments within the VLAN, enhancing security. It allows you to control your network and security environment with the ability to set very specific and granular policies in order to protect your application environment. Micro-segmentation defines rules of how applications can communicate. This will restrict communication only to hosts that are allowed to communicate. Micro-segmentation gives administrators the ability to put a wrapper around access control for each component of an application. Nowadays, you can no longer secure applications just by permitting or denying on a source destination port, or even higher up in the stack such as HTTP. Micro-segmentation gives administrators the control to set granular policies. The policies will restrict communication to hosts that are only allowed to communicate. This offers a one-to-one mapping, unlike within a VLAN where there's a potential to see everything within that VLAN. If a bad actor gains access to one segment in the zone, they're prevented from compromising any of the networks within that zone. They simply can't see them. You can't attack what you cannot see. Micro-segmentation ensures that everyone is doing what they are entitled to do, and nothing else. For effective security, you want to produce unnecessary crosstalk to an absolute minimum, and only allow communication that is a complete necessity. This reduces the attack surface to an absolute minimum by reducing the number of devices that can communicate at any given segment. Instead of using IP addresses as a base for segmentation, policies are based on logical attributes such as identity and other certificate, a tag, or a label. These logical attributes are then used to set policies that will govern application communication. If you're using a certificate, you can extend further and look inside the actual payload. For example, you can force a policy, claiming that a specific application can only do a HTTP POST to an example bidding record, but if it attempts to do anything else, it will get blocked. One of the most important aspects to keep in mind with micro-segmentation solution is that it continuously monitors the baseline for any bad behavior, such as irregular traffic patterns or communications to suspicious URLs. If you are doing this type of monitoring of the baseline, then the visibility needed for micro-segmentation needs to be in real time. A static snapshot of the application architecture, even if down to a process level, will tell you nothing about behaviors that are either sanctioned or unsanctioned. For a start, you need visibility. And not just visibility at a traffic flow level, but at a process and data contextual level. Without this level of granular visibility, it will be impossible to map and fully differentiate normal traffic flows from irregular communication patterns. It also needs to be done in real time, and also all automated. A static snapshot of the application architecture will not provide much information about behaviors. It cannot be done the manual way either. The visibility cannot be manually mapped out. Manually mapping out application traffic patterns is error prone and very inefficient. One thing you need to make sure is that you're not under-segmenting. Micro-segmentation must manage communication workflows all the way to layer 7 of the OSI layer. If you're only segmented on layer 4, which is a transport layer, you're widening your attack service to a network for compromisation. As already mentioned, nowadays we have a big problem with lateral movements within the network. If a bad actor compromised a device in a zone, and if the network is not properly segmented, they can move laterally to compromise other devices within the same segment. Micro-segmentation puts a complete lockdown on any lateral movements, thereby eliminating many well-known network-based attacks, including server scanning, denial of service, SQL injection, application vulnerability exploits, and man-in-the-middle attacks. There are a variety of micro-segmentation vendors out there, and they all have competing architectures. We have, for example, SDN-based, network-based appliance, be it physical or virtual, and container centric, just to name a few. We have the concept of inside and outside the network. Users outside of a network cannot access applications internal to the network. The way to gain remote access to internal applications from outside of network is that users would connect with a virtual private network through a security client, for example, a VPN concentrator. That is located in the DMZ, that is deployed in the central datacenter. Security clients added to the WAN do reduce the risks involved to remote access, but unfortunately they do not overcome the disadvantages, such as policy synchronization, operational issues, isolation limitations, and poor user experience. The WAN VPN architecture is not the best place for network security. Why? Because it was designed for connectivity, certainly not for security. The traditional VPN model for remote access is very much a site-centric topology approach. However, with the increase in remote workers literally working from all over the world, we really need to move away from this site-centric topology for VPN access to an architectural model where the perimeter moves with the user. We should design a network where there is no concept of inside or outside from a user's perspective. They simply don't care and should not care where the applications are located. When connecting, the users should not be concerned about where the applications are. All they want to do and care about is access to application. For this to happen we need to make applications available everywhere, without the user being required to do anything. And this is what software-defined perimeter is all about. As software-defined perimeter is part of the Zero Trust movement, a sufficient level of trust needs to be established before users can access an application, and then this trust is continuously monitored throughout the duration of the user activity. It's really important to know that this trust is continuously monitored, it's not a once-off authentication check. Software defined perimeters are really changing the way organizations look at their existing VPN architecture. VPN access to corporate assets is not a luxury. VPN access is a necessity, so it needs to be done correctly. But the traditional way of VPN access does not provide the best security and network architecture to match today's digital world. Firstly, they follow a site-centric topology with a broad level of trust. With traditional VPN's network access, initially there's too much trust. Once a user lands in a VLAN, they have the potential to see and access all other devices on that segment. You may recall that a host can send out a broadcast ARP packet to check to see if there's anything connected to that segment. Also, traditional VPNs introduce a lot of complexity. What do you do when you have multiple sites that users need to access applications in? With this type of scenario, the cost of management is very high. Users will have to make many changes to the VPN client software to gain access to applications in different locations. Traditional VPNs are complex for administrators to manage, and for the users to operate. Poor user experience that is most likely to surface as you'd need to backhaul traffic to a regional datacenter and have the user choose from a list of VPN gateways that are used for different applications. You can never win when it comes to latency. You simply can't show bandwidth to solve a problem, and if you have to backhaul traffic, you're never going to be on the right side of latency. There are a number of ways to implement software-defined perimeter. Some vendors use agents, others have an agentless approach, and then some offer as a cloud service. We can't examine every approach in this module, so let's just have a look at the cloud service to software-defined perimeter. A cloud-based software defined perimeter is an approach that consists of strategically placed software-based points of presence that will certainly help and improve customer experience. A cloud software-defined perimeter service is where you have software-based PoPs strategically placed located throughout where the users can connect to. This is in comparison to positioning the datacenter in the middle where the users have to VPN into to access that specific application. This is a site-centric topology approach to VPN access. When we look at a cloud-based approach to SDP, the user is now the center of the network. This enables the network and security perimeter to follow the user regardless of their location. The important point to note here is that software-defined perimeter provides a perimeter that follows the user regardless of their location. Instead of having a static perimeter with clear network and security demarcation points, we now have many small perimeters that follow the user around. In the near future we're likely to witness a major shift in how perimeters will be designed. There will definitely be a shift and an increase in number of perimeters. The perimeters will also become more granular, shifting closer to the logical entities that they need to protect. Moving from the traditional VPN architecture to a software-defined perimeter for VPN access completely reverses the network and security model for the better. Every house where someone lives has an address, so it can be located so friends and family can visit. Imagine that the physical address of the house to be equivalent to an IP address, and the logical address to be equivalent to a room or floor within the house. Today you're allowed to leave your home and visit any house you want, there are no restrictions. You just get in the car, drive down the highway, and have the ability to knock on anyone's door. However, you may not have the keys to open a door. But someone can wait for a vulnerability to occur, such as an open window to gain access. This is similar to a bad actor patiently waiting to penetrate a network. Zero Trust Networking states no one is allowed to even leave their home until they have prior authentication and authorization to get to that destination. With Zero Trust Networking, we state, I don't even want you to knock on my door. In this course we covered a lot of new groundbreaking material. We even discussed removing IP addresses and replacing them with names. The Zero Trust movement brings with it many new concepts that change the way we need to think about networking and security. Our environment is changing, and we can't stop this, so we need to evolve our networks to match today's environment. If not, the bad actor will always win, and right now they're winning at an alarming rate. We no longer have a static network and security perimeter, traditional firewalls and NACs fall short. However, there are many ways we can combat this, so we need to change our approach to networking and security. One way is to make IP routing more intelligent so that it can be integrated with other services such as IAM. Other ways are move to micro-segmentation and software-defined perimeters. I hope you enjoyed this course, I thoroughly enjoyed preparing it for you. Expect more modules from me in the near future regarding Zero Trust Networking.