Understanding How Zero Trust Networking Works

The digital age has introduced significant changes to both cloud and datacenter environments, which has made us look at networking and security differently. Both networking and security must keep up with these new environmental changes. If you cannot match the speed of the digital age, then bad actors will always be a hazard. So previously we discussed why we needed to move to Zero Trust approach to networking security. We also reviewed some of the options that can be included in a Zero Trust environment. But now it's time to answer the question. What exactly is Zero Trust Networking? In this module, we're going to dive into details of what Zero Trust actually is. We will focus on the path we took to get to a Zero Trust environment, and why we needed to take that path. When we examine the past, it's obvious that we've made huge progress in the evolution of our thinking regarding networking and security. For example, we've gone from single-factor authentication to multi-factor authentication. Non-encrypted traffic and motion, to encrypted traffic and motion. These changes have brought significant advantages to organizations. However, there is one additional leap we need to make, and that is to operate our networks with a Zero Trust approach to networking and security. Zero Trust starts with a security posture of default denied. Nothing is trusted either internal or external to the network. Everything, whether inside or outside, is beyond the domain of trust. Essentially, nothing in the network is trusted. Literally, you trust nothing, and then you start to open up what's known as a whitelist policy rule set, as opposed to the legacy blacklist policy rule set. The whitelist rule set can get as granular and dynamic as you need it to be. This takes segmentation all the way to the absolute endpoint of every user, device, service, and application on the network. Trust is then assessed at the initiation of network connectivity when entities want to communicate with each other. This trust ensures that both entities are doing what they're meant to be doing. Basically, with a Zero Trust network, you could say initially that the network is completely dark. Any network resource, either internal or external to the network boundary, such as a device, end-user application or service, cannot see or act as anything on the network until they have passed certain security controls. These security controls will vary depending on, for example, device type or employee. Essentially, every session that is initiated must be authenticated, authorized, and accounted for. All network sessions must go through this process prior to allowing the source and destination to communicate. Zero Trust Networking locks down all aspects of a network inside and outside of traditional firewalls. Simply put, nothing is trusted. Never trust, always verify. No UDP or TCP session is permitted to be established without prior authentication and authorization. So in summary, the Zero Trust approach to networking security assumes that nothing is trusted, either internal or external to the network. It's only once the entity's passed certain security controls that they're allowed to communicate. Zero Trust uses a whitelist approach to security as opposed to the legacy blacklist approach. We keep talking about trust, but what is trust in the world of Zero Trust Networking? Trust is the bidirectional belief that is established and maintained between two entities. It ensures that each entity is doing what it should be doing and is behaving in the expected ways during the duration of the interaction. And with Zero Trust, you would have expected by now that the default security posture is one of no implicit trust. With Zero Trust Networking, for an entity to communicate with another entity, and to be trusted, it needs to pass certain security controls. These security controls are not a once-off authentication check. They are continuously checking for anomalous behavior. There is a constant security check between these two entities. Essentially, the Zero Trust offers a one-to-one segmentation that ensures that the least privileged access. This type of continuous security trust check reduces the attack surface available to bad actors to an absolute minimum. The key Zero Trust projects at the moment include micro-segmentation, and software-defined perimeters. Software-defined perimeter is an alternative to VPN architecture, and micro-segmentation further segments networks to minimize and contain any type of breach. I'm sure there's going to be more added to the list in the near future, such as remote browser isolation, which is Zero Trust when surfing the internet. The power of RBI is that users see a normal browser user experience, except it doesn't happen on the user's endpoint device. Actually, the browsing is done on a remote server. This reduces the attack surface on the end host device to an absolute minimum, and it stops everything, both known and unknown threats. The foundation for Zero Trust environment is that nothing can be trusted. It starts with the premise that no single session, either TCP or UDP, will be allowed to be established and then starts to build a whitelist rule set from there. Previously we used legacy blacklist rule sets, but Zero Trust uses a Whitelist rule set. Initially, everything is untrusted. Let's discuss what a Black and whitelist rule set actually is. Traditionally, once a user is connected to the network, they're connected to everything that is connected to that segment. The blacklist approach starts whereby, for example, VLANs and access control lists are added to restrict access to certain segments. However, it's a manual approach to security, and is often very error prone. If you misconfigure an access control list, you could potentially leave the device open for compromise. Also, every network resource on that network needs to be previously known, and the security policies must be synchronized across all the various locations. The whitelist approach to security is the exact opposite. The whitelist approach starts with a default deny all. Whitelist rules are then created to allow users, devices, services, and applications to communicate. Whitelist rules start with a default position of denying all network access, and then builds rules that specifically allow access to those network resources. Whitelist rules explicitly allow access and give the ability to allow the session to be established or denied. As all other network resources outside of the whitelist policy are isolated, anything outside of the policy cannot see anything they're not entitled to. As I already mentioned, the network initially is dark to everything and everyone, until the administrator turns the lights on. So what path did we take to get to the Zero Trust approach to networking and security? Let's first examine VLANs and some of the challenges they pose to security. In the past, we have always divided networks into various segments. This is known as zone-based networking, or VLANs. For example, you would place external partners on one VLAN, internal sales staff in another VLAN, and maybe technical teams in a different VLAN. However, over time, VLANs became to be used as a tool for security. For users in one VLAN to communicate with users in another VLAN, they would need to pass through a layer 3 device that would usually be providing some kind of security filter to either allow or deny access. However, VLANs were never meant to be used as a security tool. Initially they were designed to divide broadcast domains. Smaller broadcast domains offer better network performance. The problem with VLANs is that they're not an effective security tool. If a bad actor compromises a VLAN, they could potentially see and access all other devices within that same VLAN. This presents a pretty large attack surface for a bad actor to play with. The attack surface really defines how susceptible and open a network is to a bad actor. The smaller the attack surface, the better, as they can do less damage. Within the VLAN, a host can send out a broadcast or a packet to see if anything else is on the network. But because it's a broadcast packet, it gets sent to a special MAC address and all devices on that segment receive and process this packet. Now this represents a substantially large attack surface, so VLANs don't really work when it comes to security, which is why organizations need and should move to micro-segmentation.