Creating a New Network and Security Model

In this module, I will introduce some of the options you can use to create a new network and security architecture. These are just guidelines for what you can use to combat today's ever-changing threat landscape. You will need to make a number of changes to traditional networking and security architectures for this to occur. First and foremost, layer three routing must become more intelligent so we can add more services to it. So what does this actually mean? IP forwarding by itself has no adaptability. It needs to be told what to do by what's known as a routing protocol. The routing protocol can be dynamic or static. A dynamic routing protocol could be, for example, OSPF, and a static routing protocol could be static routes. IP has not changed over the last decade. It operates as a standalone function, and is not integrated with any other services that could make it more intelligent. Essentially, IP forwarding is stateless. This means that no session information is retained. It is not aware of traffic patterns or data flows, and only provides location information between the source and the destination. At the moment it operates at layer 3 of the Open Systems Interconnection model. This layer is pretty low down in terms of intelligence. Layer 3 of the OSI model does not manage any state or sessions that are needed to make an intelligent network. All of the intelligence occurs higher up in the OSI model, certainly not lower down at layer 3. Additional network and security functionality devices, such as firewalls or obtrusion detection prevention systems that operate higher up in the OSI model, are added to make networks more intelligent. These devices are commonly known as middle boxes. But the foundations of IP forwarding still cannot manage any state or sessions. Currently, there are two routing focuses just on connectivity from source to destination. It doesn't examine anything higher up in the OSI stack to make its forwarding decisions. To make IP routers more intelligent and add more value to networking, we need to move them higher up in the OSI model to layer 5. Layer 5 is known as a session layer. It is responsible for many critical functions, such as encryption, anomaly detection, and identity management, just to name a few. The session layer is a really important layer in the OSI model, and is probably the most critical layer of this model. It provides a state and security for lower level network functions. The session layer opens, closes, and manages the sessions between end users and their applications. It provides more granular network and security controls for application services. The sessions are themselves stateful and end to end. Stateful means that a device can watch the data streams end to end. So instead of having the middle boxes such just firewalls everywhere, making the network more intelligent, the actual IP routers that are currently working at layer 3 of the OSI model must provide these intelligent functions natively. This is why layer 5 functions of the session layer need to be added to IP routing to create an intelligent network for a Zero Trust architecture. Layer 5 is the foundation for an intelligent network. To effectively move to a Zero Trust environment, this is where routing should be, at the session layer of the OSI model. If you want to make IP routing to work with services such as Identity and Access Management directories, the network must become more intelligent. The network must be able to maintain state. We have other devices in the network to maintain state such as firewalls and load balancers, but as already mentioned, IP routing by itself does not maintain any state. IP networks are stateless by design, which means they lack intelligence. This is not a design flaw. It was done on purpose to suit the requirements of that time. But a lot has changed since then. The reason IP routers were designed to be stateless was so that they could be fast and quickly route packets from a source to a destination. However, by adding intelligence to state to IP routers, we can then add more intelligent services to the IP devices. By adding additional services to IP routers, you can make it do more intelligent things. Identity and Access Management is a necessity for every organization. Every organization had identity stores that define entitlements of users to what they can access to. IAM consists of a set of policies and technologies that ensures the proper entities within the network have appropriate access to the resources they are requesting access to. The NAT devices do use AAA services for users that are trying to gain access to the network. But as we already discussed in module 2, it falls short in assumption that it assumes a trusted internal perimeter. However, with over 80% of attacks coming from internal to the network, this is a dangerous assumption. And Zero Trust network architecture assumes that nothing is trusted, either internal or external to the network. As we already mentioned, IP networking by itself is pretty simple. The routing rules that govern the direction of packets reside solely within the router. They interconnect networks so the endpoints can communicate, but that's about it. In today's world, IAM and IP routing are not tightly coupled. What this means is that they're not integrated and work with each other. IAM is used to grant access for end users to get on to the network, but it cannot affect how packets are routed from one source to a particular destination. IAM does not influence how packets should be forwarded. There is a complete lack of integration between routing protocols, such as BGP and OSPF, with Identity and Access Management services. Zero Trust changes all this. Zero Trust combines the routing tables of IP routers, which display the source and destination. But along with the policies of an IAM directory, this adds more intelligence to the network because now the policies of the directory are used to allow or deny a packet to go from one source to a particular destination. By adding IAM services to IP routing, it creates a more intelligent network that can provide more dynamic and granular security controls that are needed for today's digital world. Malicious traffic must be stopped at the edge of the network, not in the middle or in the end host where it can cause the most damage. Bad actors have a process that they follow. The process they follow involves discovery, identify, target, and then attempt to compromise an organization's valuable assets. They usually do data exfiltration, meaning that the bad actor takes data out of the organization, maybe even via Twitter or a DNS account. To stop this, we must push all networking and security functionality to the absolute edge of the network. This will stop the bad actors from even initiating the processes that lead to an attack. The edge of the network is where communication starts, so it makes perfect sense if the traffic is malicious that it should be stopped there. When you push the routing and security functionality to the absolute edge of the network, it minimizes the available attack surface available for bad actors to an absolute minimum. You could say that they have no available attack surface to play with. No attack surface, therefore, no damage to valuable assets. Why would you want to allow malicious traffic into the network anyway? By design, we've always had a breachable perimeter. The traditional network perimeter never really worked, and it was only a matter of time before a bad actor could breach it. Zero Trust ensures that security policies are applied right at the edge of the network and stops malicious traffic right at its origin, not in the middle or at the end point. The edge of the network is where the network sessions are established, so Zero Trust stops all malicious sessions from establishing unless they are explicitly allowed to. With this approach, bad actors simply have no way to gain access into the network and the resources that lay within it. Another option is to use names and not IP addresses for identity. Back in the days, networking was designed to connect things easily with IP addresses, but a lot has changed since its inception. Networking has evolved to be dominated by a content distribution and retrieval network. Data is decor, and we live in what's known as an information-centric world that is driven by, for example, mobile digital media and social networking and video streaming. The core problem is that IP networking is location based. Everything has an IP address, and defines the where, the location. However, we live in an information-centric world. The networking protocols we use today still focus on the connection between hosts, the source and the destination, but not on the data. Users now expect to find a what, the data, but the current communication model for networking is still focused on the where, which is the IP address. The most obvious solution is to replace the where with the what, and this is what named data networking proposes. Named data networking proposes evolution of the IP architecture so that packets can name objects other than communication endpoints. Named data networking started in 2010 as a National Science Foundation research project. That was used to create an architecture for the future internet. It completely changes the paradigm used by traditional networks. Instead of delivering a packet to a given destination IP address, we are fetching data identified by a given name at the network layer. Fundamentally, named data networking doesn't even have the concept of a destination, whereas in the world of IP, the destination address is used to guide the forwarding of traffic towards that destination. However, with NDN, there simply is no IP addresses. The NDN network layer uses application data names to communicate instead of IP addresses. So at this moment, I guess you're saying, Matt, so I get it. You're telling me to use names instead of IP addresses. But why? Networking has changed a lot over the last 30 years. Now it's all about data, but IP addresses is all about connecting one endpoint to another and doesn't even look at the data. Also, NDN has a state for forwarding data claim for datagram delivery, per packet and per hub in comparison to IP's stateless forwarding pain. It goes beyond traditional paradigm and adds intelligence and state to each device. With NDN, the name is used to guide the forwarding and not the IP address. In the case of NDN, there may be multiple devices that can hold the requested data. But with IP addresses, there's usually only one destination. And in the IP world, if you were sent the datagram, you'd better be able to deal with it and handle traffic that you're announcing. NDN routes and forwards packets based on names, which eliminates problems such as IP address space exhaustion, map transversal, IP management, and even upgrades to IPv6. Think of a network as a country. Within that country, there are both public and private places that people are allowed to go to, depending on who they are and what they want to do. People within a country are provided with a means of identification, such as a driving license or social security number. People from outside the country must validate themselves through customs before they enter that country. You need to hold a stronger identification method such as a passport when you're trying to enter a country than if you're simply trying to move within that country. Determining the identity of an individual is equivalent in the rights to access that can be correlated to various zones within a network. Certain entities can access certain parts of a network based on their identity and their role. The identity of a person, for example a driving license, follows them as they travel, unlike traditional IP networks that lose identity when, for example, their IP address changes.