Network Virtualization

What Is A Virtual Network?

Before even the term "Cloud" became a household term, networks have always existed, in some shape or form. Typically, this involved hardwiring servers together, and using other hardware-based components, such as routers, switches, hubs, firewalls, etc. But given the huge and dramatic advances in technology, especially with the Cloud based platforms (such as those of the AWS and Microsoft Azure) networks can now become what is known as "virtualized".

This simply means that that of the devices and cabling that were once present in a physical form are now represented as software-based mechanisms, in a virtual form. Thus, it has been given the term "Virtual Network". The only physical component that is needed are those that will allow the IP based data packets to be transmitted from the point of origination to the point of destination, of course with the usual intermediary hops along the way.

Typically, there are two types of Virtual Networks that are used, such as:

- The External Virtual Network:

  Those networks that are physical connected together can now be connected into separate Local Area Networks, which are known as VLANs. Conversely, those physical networks that are not connected together directly can come together as one unit, or one common VLAN.

- The Internal Virtual Network:

  Typically, these are found on Cloud based platforms, and only one Virtual Machine (VM) is needed to control the entire network. This is the opposite of the above scenario, where there could be multiple servers that are involved.

There are numerous benefits in using a Virtual Network, and some of these strategic advantages include the following:

- There is hardly any hardware that is required;
- It allows for the workloads to be flexible as and when needed;
- It can permit for drastic increases in workload provisioning if the business environment warrants it;
- Easy scalability is huge here, as network resources can be increased and/or reduced in just a matter of a few seconds, as needed.

How Virtual Networks Can Be Used To Secure Resources

Apart from those just described, one of the other greatest benefits that a Virtual Network can bring to a company is that of securing the shared resources and assets. Here is how it is done:

1) Isolation:

   Although the Virtual Networks may be interconnected together in the Cloud, the bottom line is that there are still isolated from one another. They are also separate from the other pieces of physical hardware if there are any. With this in mind, it is quite east to thus deploy what is known as the concept of Least Privilege. This is the situation where you only give your

employees the bare minimum of access rights in order for them to conduct their daily job tasks. By default, Virtual Networks are typically set up this way, unless you make other changes in the configuration settings. Usually, Cloud based infrastructures are hosted in a shared environment, where all of the tenants in one physical server make use of the same processing and computing resources. Because of this, there is the risk that leakage from one tenant could be spilled over into the others. But the isolation of the Virtual Networks greatly mitigates from this from actually happening.

2) Segmentation is easier:

Given the Cyber threat landscape of today, many businesses today are now opting to divide their entire network infrastructure into multiple ones. This process is technically known as segmentation. So rather than having just one main network, there now multiple ones, which are referred to as subnets. In a way, this is like adopting the Zero Trust Framework, in which multiple zones defense are created. The main premise here is that if a Cyberattacker were to break through one Virtual Network, the statistical probability of them breaking through the others and reaching the crown jewels becomes almost nil. Also, there can be micro subnets that can be created in one main subnet, with each of one of them serving a different purpose, known as tiers. For example, one could serve the needed resources for the web server, the other could provide the resources for the database, etc. Although this may sound complex, it is actually very easy to configure and deploy when using a Virtual Network. Further, this approach adds even more redundancy in terms of security.

3) Advanced tools can be used:

When making use of a Virtual Network, much more sophisticated tools can be created and deployed to help enhance the levels of security in your Cloud based platform. For instance, many Artificial Intelligence (AI) and Machine Learning (ML) packages can be easily inserted in the lines of the Virtual Network on a real time basis. The bottom line here is that you will be able to enforce, distribute, and enable far superior threat monitoring services into your Virtual Network as opposed to using a Physical Network. Also, any policy changes or updates that you make to your overall Security Policy will be quickly reflected.

4) A more balanced approach is taken:

As mentioned earlier, many organizations are now opting to move entirely over to the Cloud. But there are still those that are opting to stay with their On Premises infrastructure. In this regard, a Virtual Network will allow for an equal balancing of resources in both kinds of environments. So, if a company decides to take this hybrid type of approach, the Virtual Network can easily pick up the slack where the Physical Network may be failing at. For example, if there is a point at which there slow downs are bottlenecks are becoming a problem in the Physical Network, that part could be provisioned over to the Virtual Server to eradicate this issue in just a matter of a few seconds.

Conclusions

Overall, this article has examined what a Virtual Network is, and the benefits it brings in protecting your Cloud environment. Although deploying it can be done in a short amount of time, it still takes careful

planning. After all, you don't want to have any downtime in your network infrastructure, both from the Cyber and productivity standpoints. If you have more questions on this, please contact us today.

Sources

1) https://www.vmware.com/topics/glossary/content/network-virtualization
2) https://www.redhat.com/en/topics/virtualization/what-is-network-virtualization
3) https://www.infoworld.com/article/2609571/4-ways-network-virtualization-improves-security.html