T2022_08 How Can Segmentation Help Secure Your Network (16th May 2022)

What Is Network Segmentation?

Segmentation is used by businesses to increase monitoring, performance, pinpoint technical faults, and, most critically, security. It is a technique that splits a network into several segments or subnets, each of which functions as its own separate network. This enables the network managers to use flexible policies to govern traffic flow between subnets.

Network segmentation can be used for a variety of applications, such as:

- Guest wireless network
- User group access
- Public cloud security

What are some advantages achieved through Network Segmentation?

Among the many benefits of network segmentation are:

Slowing Down Attackers: During an attack, network segmentation can buy you time. If an attacker successfully compromises your network and it is segmented, it will take the intruder some extra time to break out of the segmented area of the network.

Increasing Overall Data Security. It becomes easier to protect the most sensitive data on your internally facing network assets by segmenting networks. The implementation of a layer of isolation between servers carrying sensitive data and everything beyond your network can minimize the risk of data loss or theft.

Enabling the Implementation of a Least Privilege Policy. Strong network segmentation makes limiting user access to your most critical data and systems much simpler. Network segmentation can help you safeguard your company from both insider and outsider attacks.

Reducing Damage from Successful Attacks. Strong network segmentation can assist mitigate the harm caused by breaches, preventing attackers from getting out of a system before you've isolated the breach and turned off their access.

Improved operating performance. Traffic is restricted to specific zones. This minimizes the number of hosts and users on each subnet, reducing congestion and improving overall Network performance.

The scope of compliance has been narrowed. Segmentation separates regulated data from other systems, making it easier to manage compliance

Tips for Segmenting your Network:

- Inventory management systems determine the classification and location of sensitive data. Ask yourself, what exactly do I have? Who has access to it, and how?
- Identify and group systems and data classifications that are similar.
- Determine who requires what data, This is because access is only granted to only those who require it.
- There are several methods for segmenting your network. Firewalls, Virtual Local Area Networks (VLANs), and Software Defined Networking are commonly used to segment networks (SDN).

- VLAN segmentation: VLANs or subnets are commonly used to divide networks. VLANs are virtual network segments that link hosts together. IP addresses are used to divide the network into subnets, which are connected by networking devices.

- Segmentation using firewalls: Firewalls are another approach to enforce segmentation. Inside the network, firewalls are used to create internal zones that separate different functional areas

References

Dosal, E. (2019, November 26). *What Are the Benefits of Network Segmentation? Retrieved from compuquip.* Https://Www.Compuquip.Com/Blog/4-Security-Benefits-of-Network-Segmentation#:~:text=By%20segmenting%20networks%2C%20it%20becomes,Of%20data%20loss%20or%20theft. https://www.compuquip.com/blog/4-security-benefits-of-network-segmentation#:%7E:text=By%20segmenting%20networks%2C%20it%20becomes,of%20data%20loss%20or%20theft.

Turner, J. (2022, March 10). *7 Network Segmentation Best Practices to Level-up.* Retrived from strongDM. https://www.strongdm.com/blog/network-segmentation

What Is Network Segmentation? Retrieved from paloaltonetworks https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation