An Introduction to Micro-Segmentation

A Brief History

For many years it has been well known that corporate networks carry a lot of different types of traffic, and this traffic may be subject to different levels of security requirements. Traffic within a DMZ is typically less trusted than an internal server subnet for example. The use of VLANs has exploded to segment the network into different zones to separate different applications and application tiers from each other, with each VLAN requiring traffic to pass through a firewall to be policed. This complexity often meant traffic having to take a convoluted route to be policed between VLANs at a firewall, and overly complex network architectures. The biggest flaw with using VLANs to segment a network is that if a single machine within the VLAN is breached, there is nothing to stop a hacker from attacking all the other machines on that VLAN. A ransomware outbreak, for example, could spread and wipe out all your web servers for instance, not just one!

'Zero Trust'

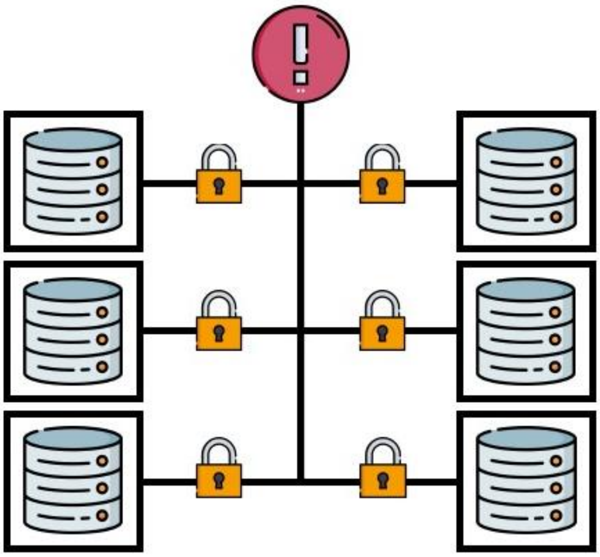
More recently, the zero-trust paradigm has become more widely adopted. Instead of building walls around the outside of your network, the concept is that you should treat your internal networks as inherently unsafe – just like the internet. This means protecting your assets closer to the source, removing the soft underbelly, prone to attack that VLANs help to create.

Micro-segmentation is one component of the Zero-Trust methodology. Taken to its extreme, it can reduce the size of each segment to just a single host – meaning that its no longer possible to compromise an entire organisation with the breach of a single machine. Every machine has protections built around it, and each must be individually breached, making the attackers job impossible – or at least slowing the attack down such that you have time to detect and remove them from the network before harm is done.

Types of Micro-Segmentation

Software Defined Networking (SDN) Based Micro-Segmentation

This method relies on a software defined networking infrastructure to control flows across the network. The SDN controller manages all flows, therefore can programmatically permit or deny flows based on a defined ruleset. SDN based micro-segmentation is a good fit for relatively static private cloud deployments but can't protect dynamic hybrid cloud deployments with mobile and temporal workloads. This type of micro-segmentation can introduce chokepoints that may impact network performance and complicate network engineering. An example vendor in this space is Cisco, with their Application Centric Infrastructure (ACI) platform.



Hypervisor Based Micro-Segmentation

This mode relies on the low-level controls provided by the virtualisation hypervisor to direct traffic. Typically, this is an add on to the core virtualisation software which acts in a similar way to the SDN controller in the previous method. This method is worth considering if you are committed to the virtualisation vendor and the entire estate is in scope for virtualisation. Conversely, hypervisor-based micro-segmentation may not be a good match for organisations using bare metal workloads, heterogeneous cloud and server virtualization technologies as it may not support these other environments or provide protection for mobile workloads that migrate outside of the hypervisor domain.

Host Based Micro-Segmentation

Rather than delegate micro-segmentation to the network, some organisations opt to collocate security controls with the workloads themselves. In this way, policy enforcement rules live beside the assets that need protection, which is a security best practice. Host-based micro-segmentation is especially useful for mobile and temporal workloads because micro-segmentation rules can be programmed into the hosts when provisioned and then remain with the workloads regardless of location or duration. Host-based technologies can be complex as they introduce the need to manage policy and enforcement rules for hundreds or thousands of workloads rather than a few centralized networks or hypervisors.

Armadillo Recommendations

Host based micro-segmentation should be considered as the default mode of micro-segmentation. The constraints of typical host-based firewalls has now been removed with centralised controllers that not only provide the ability to manage the estate as a whole, but provide until now unprecedented visibility into the data flows around your network.

If you have ever had to plan a data centre migration, a move to the cloud, or divest part of the business and it's associated IT estate, you will be well aware of the complex, interconnected nature of a modern data centre. With modern tools, you can visually depict all the flows between production and non-production environments, between applications, between different tiers of an application, and even between two servers in the same tier.

Micro-segmentation should be considered for the following use-cases:

- Reducing complexity in environments that have become unmanageable due to over use of VLAN segmentation
- Increasing security in networks where flat VLANs are common
- Reducing the risk of lateral movement after a breach
- Providing visibility into complex networks of interconnected applications, especially as a precursor to a migration or divestiture
- Providing support to the rollout of new applications in complex environments where often the communications flows are not clear
- Reducing expenditure of firewalls – both in terms of capital hardware and software costs, but in terms of ongoing management
- Building flexibility and agility into your security stack – allowing security to support the DevOps model.