xtravirt

An introduction to micro-segmentation

Transforming network security inside the data centre

As networks make the transition to software, the security used to protect them must also move from physical to virtual.

Remaining resilient is one of the biggest challenges facing organisations today especially in a world where cyber threats are increasingly putting commercial operations and business reputation at risk. Micro-segmentation as an approach to data centre security is becoming the leading solution to mitigating cyber threats. Network security inside the data centre is significantly transformed by micro-segmentation as it builds security from the inside out.

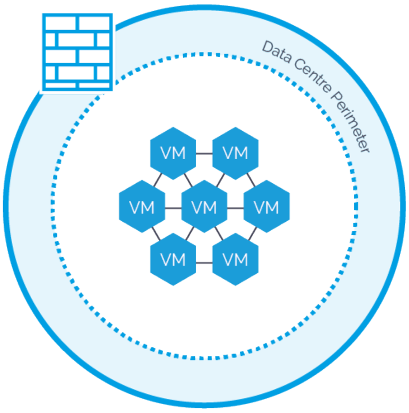
> *"Micro-segmentation refers to the practice of splitting up a unified system into many isolated segments. Micro-segmentation in IT refers to the practice of creating secure zones in data centres and cloud deployments, thereby enabling workloads to be isolated from one another and individually secured. It provides a more granular approach to network security than traditional perimeter-based security measures. Using Software-Defined solutions such as VMware NSX™ enables the east-west traffic flows inside the datacentre to be protected."*

Micro-segmentation is a security solution that enables fine-grained policies to be assigned to data centre applications down to the workload level. This approach enables security models to be deployed deep inside a data centre using a virtualised software only approach.

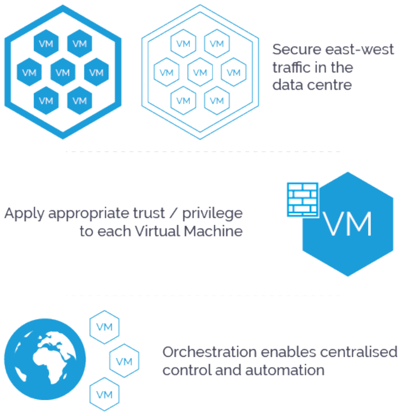
With micro-segmentation, security settings can be tailored to different types of traffic, creating policies that limit network and application flows between workloads to those that are explicitly permitted.

The goal is to decrease the network attack surface. By applying the segmentation rules down to the micro level of the workload or application, the risk of an attacker moving from one compromised workload or app to another is reduced.

Traditional perimeter defence

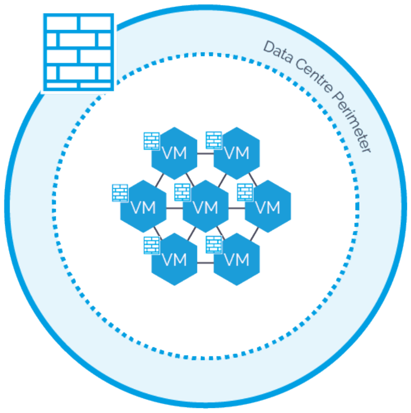


Micro-segmentation enters the picture



VM
Secure east-west traffic in the data centre
Apply appropriate trust / privilege to each Virtual Machine
VM
Orchestration enables centralised control and automation

Security can be applied per workload not just to the perimeter



Key benefits of micro-segmentation

Generally micro-segmentation is used to improve the security and efficiency of a network but the benefits to an organisation can be more far-reaching than this.

1 Minimise risk and impact of data centre security breaches

The growth of east-west (server to server) traffic generated by modern applications is continuing to grow exponentially, which in turn consumes network bandwidth, adds complexity, increases latency and over subscription on the data centre network core. With micro-segmentation, any threats that infiltrate the data centre can be contained and the lateral movement to other servers is blocked, this dramatically reduces the attack surface and the risk to the business. Because each workload is isolated with its own security policy, attackers are prevented from exploiting other systems and stealing valuable data.

2 Automate IT service delivery and accelerate time to market

In the same way that server virtualisation transformed the operational model of computing, networking has been transformed by network virtualisation, which enables micro-segmentation and transformed security in the data centre. This is allowing organisations to provision security services with the same speed, agility and control as virtual machines for computing.

3 Leverage existing infrastructure

Micro-segmentation is not an all or nothing proposition. Because virtual networks require practically no configuration changes to the underlying physical network they can transparently co-exist on the physical network with as much or little micro-segmentation of existing application workloads as needed.

Organisations can deploy micro-segmentation in their data centres at a pace that suits their specific business needs, whether in a proof of concept, a multi-tiered application or full scale SDDC build.

Organisations can use micro-segmentation and network virtualisation to bridge and simplify data centres without disruption. They can leverage their existing physical network and security equipment, and in many cases extend the useful life of their existing infrastructure.

4 Operational efficiency

Access control lists, routing rules and firewall policies can get cumbersome and introduce a lot of management overhead, making policies difficult to scale in rapidly changing environments. As micro-segmentation is typically done in software, it is easier to define fine-grained segments enabling organisations to centralize network segmentation policy and reduce the number of firewall rules needed.

5 Reducing expenditure

Deploying the additional physical firewalls to control the increasing volumes of east-west traffic inside a data centre can be cost prohibitive for many organisations, along with the number of devices and effort required to set up and manage the firewall rules. With micro-segmentation, organisations can have complete control of individual workloads in the data centre without purchasing additional firewalls for each workload, resulting in significant savings.

Along with a reduction in capital expenditure, micro-segmentation can also result in lower operating costs through a reduction in the manual effort and time required for many tasks such as provisioning, remediation, scaling and troubleshooting. The level of effort can be reduced from hours to minutes.

Considerations in adopting micro-segmentation

Using micro-segmentation to improve network security and gain more flexibility is an attractive proposition, but before you start, here are a few points to consider:

Scoping - one of the most important considerations is knowing what to segment. It is essential to know precisely what IT devices are on the network. If you don't even know what devices are on the network, how do you know what kind of segments to create?

Visibility – ensure there is a thorough understanding of network traffic flows and communications processes to, from and within the datacentre.

Analytics tools – identify relationships between different applications, vulnerable network areas and highlight points of network inefficiency.

Policy definition and orchestration system – this is vital to creating the policies needed for micro-segmentation and pushing policies out to infrastructure.

Implementation of security rules and policies – though recommended, it's not always practical to adopt a zero-trust approach for the entire estate at day one. Therefore, consider a more app-centric approach whereby you enable micro-segmentation on a per application basis and therefore apply the zero-trust principles on a per application basis.

Closing thoughts

It's clear that organisations need to re-think the security of their data centres and ensure they have the ability to defend against breaches. Network virtualisation makes micro-segmentation in the software-defined-data-centre a reality, giving organisations the ability to rapidly and securely grow while maintaining persistent security in the data centre.

Micro-segmentation is proving to be a leading solution to counter the many threats that we are seeing impacting our IT security systems today. Technological advancement, increasing use of applications, connected and mobile devices along with the increasing rates of cyber-attacks are all contributing to the growth of micro-segmentation; a market that Xtravirt predict will grow by 20% over the next 3 years. Organisations are starting to realise the many benefits of micro-segmentation as a network security solution and this will continue as uses and applications of the technology grow.

As experts in network virtualisation and micro-segmentation, and leading VMware NSX specialists, Xtravirt understand how to help organisations protect their data centres. We can work with you to advise, design, build and deploy the right solution for your organisation to help you avoid the pitfalls and plan for success. Contact us and we'd be happy to use our wealth of knowledge and experience to assist you.

Useful links

Case Study: Improved data centre security for global telecoms company

Case study: Micro-segmentation solution improves network security for web hosting specialist

Blog: European Airline uses VMware NSX with Micro-segmentation to improve IT security

Blog: VMware NSX and vRNI – a customer solution

Packaged Service: Network Virtualisation planning for VMware NSX

About Xtravirt

Xtravirt are an experienced consulting firm dedicated to delivering outcomes to help customers solve their IT challenges. We design and build strategies to help customers unlock the full potential of cloud, datacentre and workspace technology.

We are the VMware Global and EMEA Professional Services partner of the year 2017/18.

www.xtravirt.com

vmware® PARTNER
MASTER SERVICES COMPETENCY
NETWORK VIRTUALIZATION

xtravirt