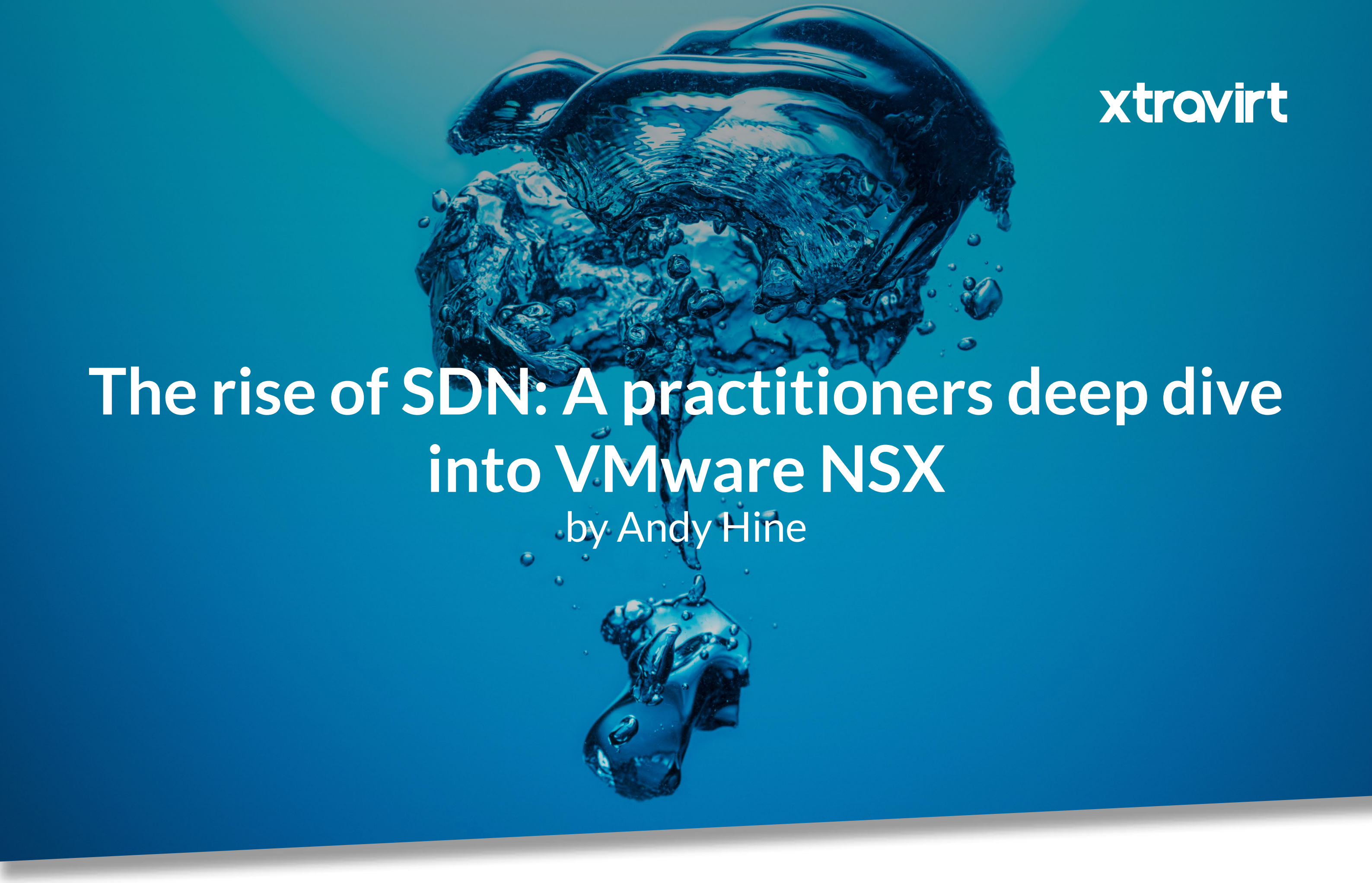


The rise of SDN: A practitioners deep dive into VMware NSX

by Andy Hine

Introduction

The hype about Software Defined Networking (SDN) has been around for years, during which time the technology has rapidly matured, leading to fast growing adoption. So what is it all about? In this article I'll share a bird's eye view at software based networking, and in particular VMware® NSX.

The areas covered are:

- What is SDN?
- Origins of NSX
- Why virtualise the network?
- Traditional network challenges
- How does NSX achieve network virtualisation?
- Features and architecture

What is SDN?

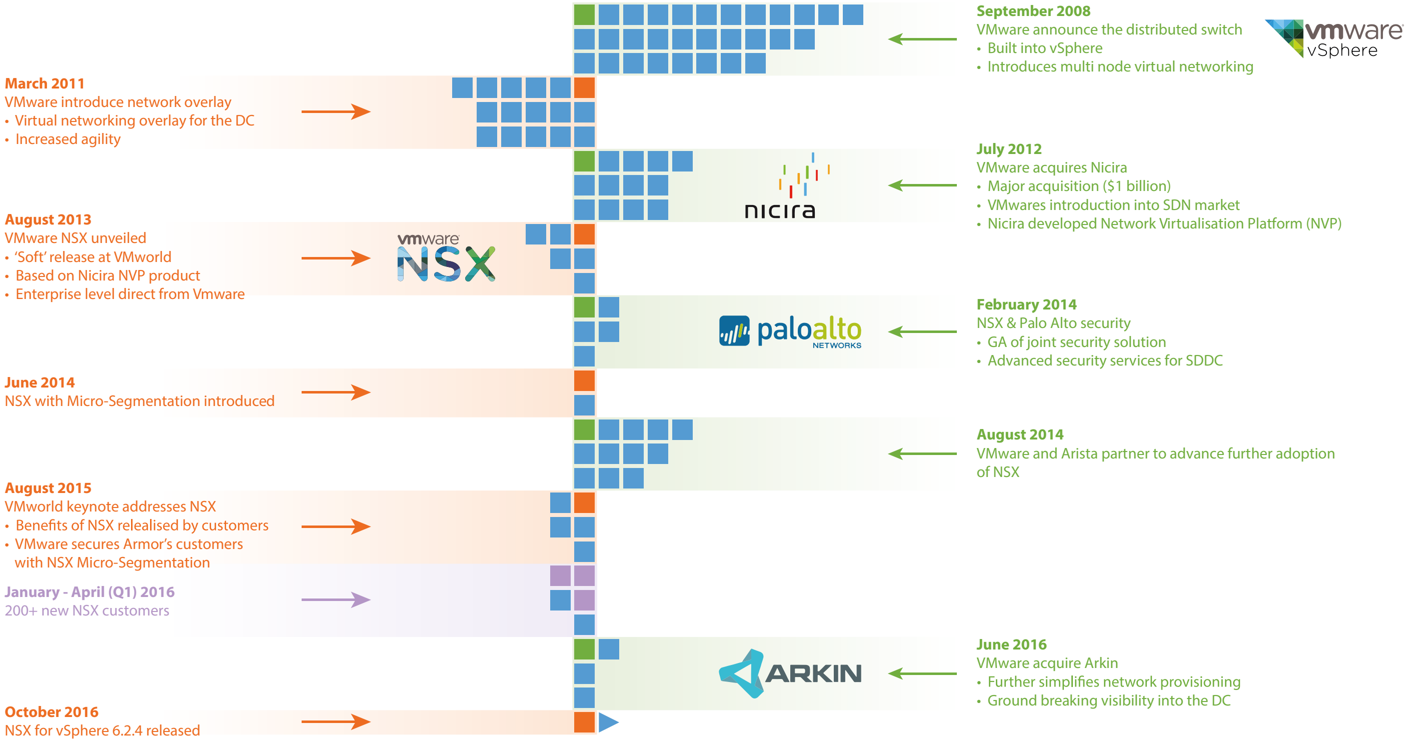
For those who have managed to avoid the marketing, SDN enables networking and security functionality traditionally handled with hardware based equipment, eg: network switches, firewalls, load balancers, to be performed in software. This process is often called 'Network Virtualisation' and involves the abstraction of networking from its physical hardware.

VMware NSX is a network virtualisation platform that VMware hope will fundamentally transform the data centre's network operational model, just like the server virtualisation 'bonanza' did over 10 years ago. This, in the eyes of VMware will continue the organisational march to realising the full potential of the Software Defined Data Centre (SDDC – a term coined by VMware a number of years ago). As part of this drive, NSX is now integrated into the later versions of VMware's vSphere hypervisor.

Origins of NSX

So where did NSX come from? Back in July 2012 VMware purchased Palo Alto based company Nicira for $1.2 billion. This represented the most expensive acquisition made by VMware (and most likely will be for a long time yet), showing how serious they were and are about their SDDC vision.

Nicira were founded in 2007 and had a modest (ish) customer base of mainly enterprise clients.. Whilst their focus was on network virtualisation and developing SDN products, most were for non-VMware and open source platforms. NSX was developed from Nicira's existing NVP software.



September 2008
VMware announce the distributed switch
- Built into vSphere
- Introduces multi node virtual networking

March 2011
VMware introduce network overlay
- Virtual networking overlay for the DC
- Increased agility

July 2012
VMware acquires Nicira
- Major acquisition ($1 billion)
- VMwares introduction into SDN market
- Nicira developed Network Virtualisation Platform (NVP)

August 2013
VMware NSX unveiled
- 'Soft' release at VMworld
- Based on Nicira NVP product
- Enterprise level direct from Vmware

February 2014
NSX & Palo Alto security
- GA of joint security solution
- Advanced security services for SDDC

June 2014
NSX with Micro-Segmentation introduced

August 2014
VMware and Arista partner to advance further adoption of NSX

August 2015
VMworld keynote addresses NSX
- Benefits of NSX relealised by customers
- VMware secures Armor's customers with NSX Micro-Segmentation

January - April (Q1) 2016
200+ new NSX customers

June 2016
VMware acquire Arkin
- Further simplifies network provisioning
- Ground breaking visibility into the DC

October 2016
NSX for vSphere 6.2.4 released

Why virtualise the network?

By automating and simplifying many of the processes that go into running a data centre, network virtualisation helps organisations achieve major advances in simplicity, speed, agility and security. With this approach to the network organisations can:

- Achieve greater operational efficiency by automating processes
- Improve network security within the data centre
- Place and move workloads independently of physical network activity

Complexity in Service Development

Manual and Risk-Prone Configuration

Capital and Operational Costs

Insufficient and Weak Security

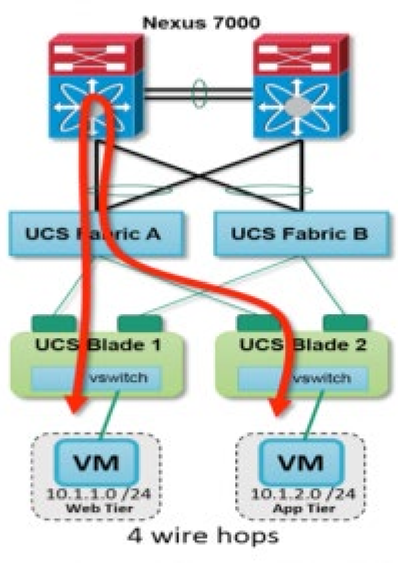
Traditional network challenges

Networking teams respond to the request for change from the business with manual and often complex provisioning of hardware devices, software and configuration. And this is usually performed by an engineer with specific knowledge of the particular technology. This can create bottlenecks in provisioning new networks and applying network related changes, along with introducing the possibility of configuration errors and even outages due to human factors.

To explain by way of example; imagine a new application is to be developed, it requires isolated test, development and production environments to support it, and each environment has its own web tier in a DMZ, and all need access to a central application library and code repository... and the deadline is yesterday. The virtualisation team have provisioned the virtual server resource and passed it over to the network team. Now what? The team manually provision new physical networks? Access ports? Trunk ports? VLANS? Firewall rules? Is there capacity on existing switches? Where is routing going to occur? Where will the DMZ be placed? And who's got the skills and time to do it? ... "This is complex...let us get back to you."

You can see how this type of commonly repeated scenario can lead to a number of other challenges. What happens if a workload needs to move from one host or resource pool to another, for example due to maintenance. Can the new destination support the networks that the VM is currently part of? Will this require a change of IP address? Will that be in the right rule base, and please don't tell us you need to move a VM from test to production. This traditional networking approach is static, inflexible and produces silos. The management overhead is increased further by sprawl of VLANs and firewall rule sets.

Years of server virtualisation has meant that IT infrastructure teams can now respond quicker to these type of business challenges, in fact they may well have a lot of their processes automated, maybe in provisioning new workloads or remediating issues, with integration into service desk and change management systems. So is there any chance the networking can follow suit? Well it's certainly slower and more complex with the traditional approach.

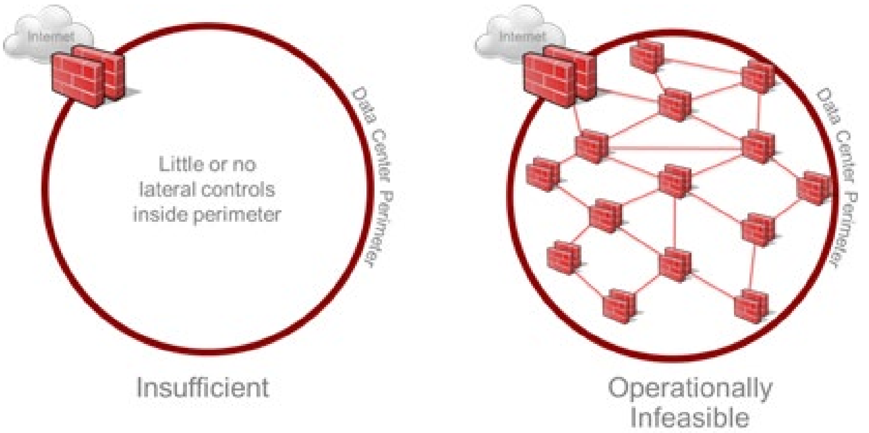


The ability to rapidly provision, update, and decommission networks (including DMZ's) in an agile, lower risk and highly available way can be achieved through network virtualisation, and is a major use case for VMware NSX. Add to that massively reduced management overhead, the ability to automate these processes and even integrate it with existing systems makes it a very compelling conversation.

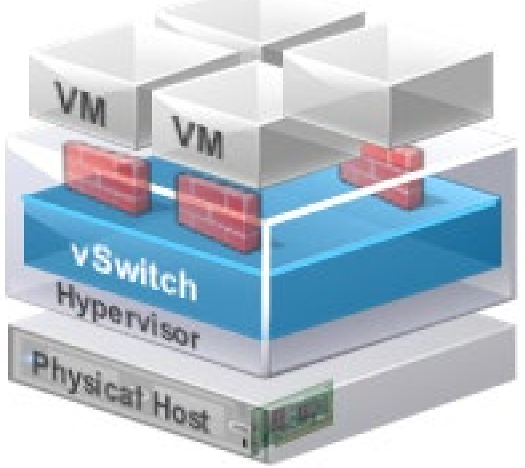
Security and routing are other networking challenges, traditionally it has been the '**Castle**' approach where IT has secured the data centre perimeter. Often achieved by having a powerful hardware device at the edge (or multiple if a DMZ is required), sporting large throughput capacity, firewalling and L3 routing capability with maybe some anti-virus or intrusion detection.

I see a couple of issues with that approach, firstly performance is a concern, causing potential choke points and inefficiency as each workload's networking may be subjected to 'hair-pinning'. The process whereby the network packet travels from the source machine all the way up to the edge device, is processed and then set off on the return journey back down again to the destination (even if the destination is located on the same physical host by the way).

As more and more of the data centre is defined in software, the transition to east-west traffic is huge. A simple example is virtual machine A, which is part of internal network 10.1.1.x and running on DC host 1, wants to communicate over TCP port 80 with virtual machine B, which is part of internal network 10.1.2.x running on DC host 2 – this is traffic that does not need to leave the data centre for any reason like north-south traffic, so therefore should not need to bother with adding extra processing at the edge device and also slowing down its own round trip time.



And what happens if a threat slips through the cracks, some malware on a VDI machine for example – how is that contained? With the Castle model, once a threat is inside it can roam around freely connecting to as much as it can, of course attempts to counter this may be with software ("personal") firewalls on each VM or having individual rules for every single machine on the perimeter device, or even having physical firewalls between each machine. None of those options are scalable or manageable, and the latter for your average organisation is nonsensical.



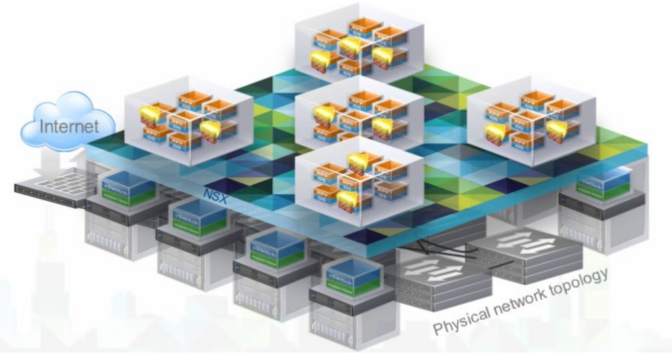
By creating granular security for network segments at layer 2 instead of layer 3, this not only allows IT to increase network efficiency and reduce chatter but also introduces firewalling to east-west traffic, establishing a much more secure zero-trust operating model for networking (even within the same VLAN).

Security can be deployed at the VM, at vNIC level. To stick with the analogy earlier we have now created the 'hotel' model. This process is called **Micro-Segmentation**, and is another major use case driving NSX adoption.

How does NSX achieve network virtualisation?

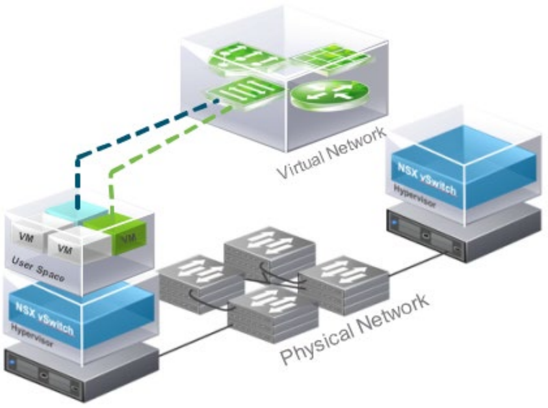
VMware NSX applies network virtualisation to the physical network, much like a hypervisor does for compute, this allows for software based networks to be created, managed and deleted.

When defining networks in software (or logically) we are providing an overlay that decouples the virtual plane from the underlying hardware rendering it a network backplane, so merely a vehicle for traffic to travel on the physical network. This introduces potential to extend the life of hardware or reduce cost of its replacement due to the transition of the intelligence into software.



VMware NSX builds upon vSphere vSwitch technology as well as adding:

- Encapsulation techniques at the hypervisor level
- Introducing new vSphere kernel modules for VXLAN
- Distributed logical routing and distributed firewall services together with edge gateway appliances to deal with north-south traffic routing
- Advanced services such as load balancing



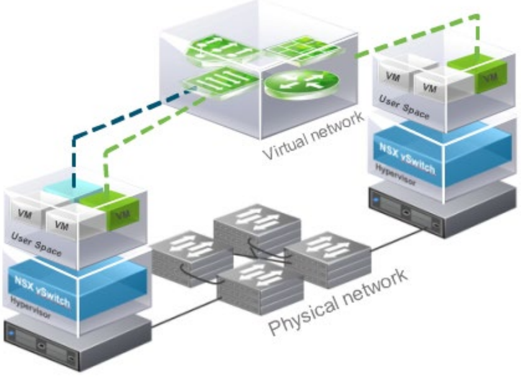
The example in the diagram above shows VMs (green and blue) on the same host but on different networks. Using NSX virtual networking services (2 x NSX vSwitches and 1 x NSX distributed logical router to be precise) the VM's can communicate with one another without a single frame leaving the host.

The diagram to the right shows Virtual machines on different hosts can communicate through NSX distributed logical switches even when the underlying physical network is not configured. In this example that would mean the network team would not have to do anything.

Features

NSX allows for networking functions previously defined in hardware to be realised virtually, including logical switching and routing, firewalling, load balancing and VPN services.

NSX also provides a REST API for integration with additional network/security products and cloud platforms.



Logical Switching
Layer 2 over Layer 3, decoupled from the physical network

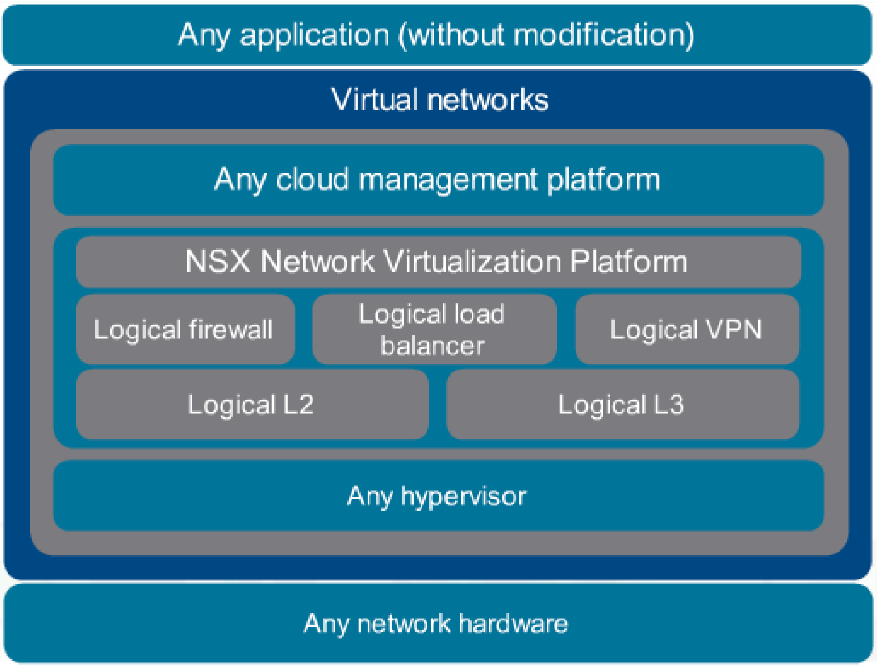
Logical Routing
Routing between virtual networks without exiting the software container

Logical Firewall
Distributed firewall, kernel integrated, high performance

Logical Load Balancer
Application load balancing in software

Logical Virtual Private Network (VPN) Site-to-Site & remote access VPN in software

VMware® NSX API™ - REST API for integration into any Cloud Management Platform
Partner Eco-System

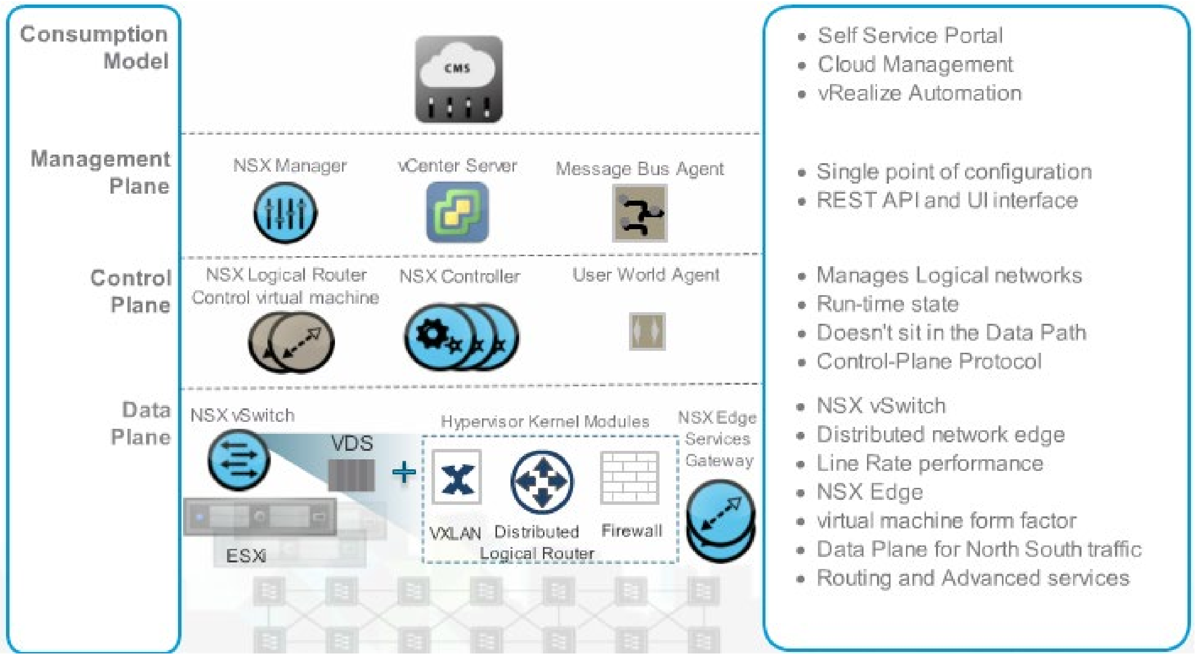


Architecture

For those looking to realise network virtualisation it is important to understand that in the case of NSX there is no single component that will 'switch on' networking virtualisation. As shown in the overview of the architecture below, there are a number of integrated technologies working together to enable its introduction.

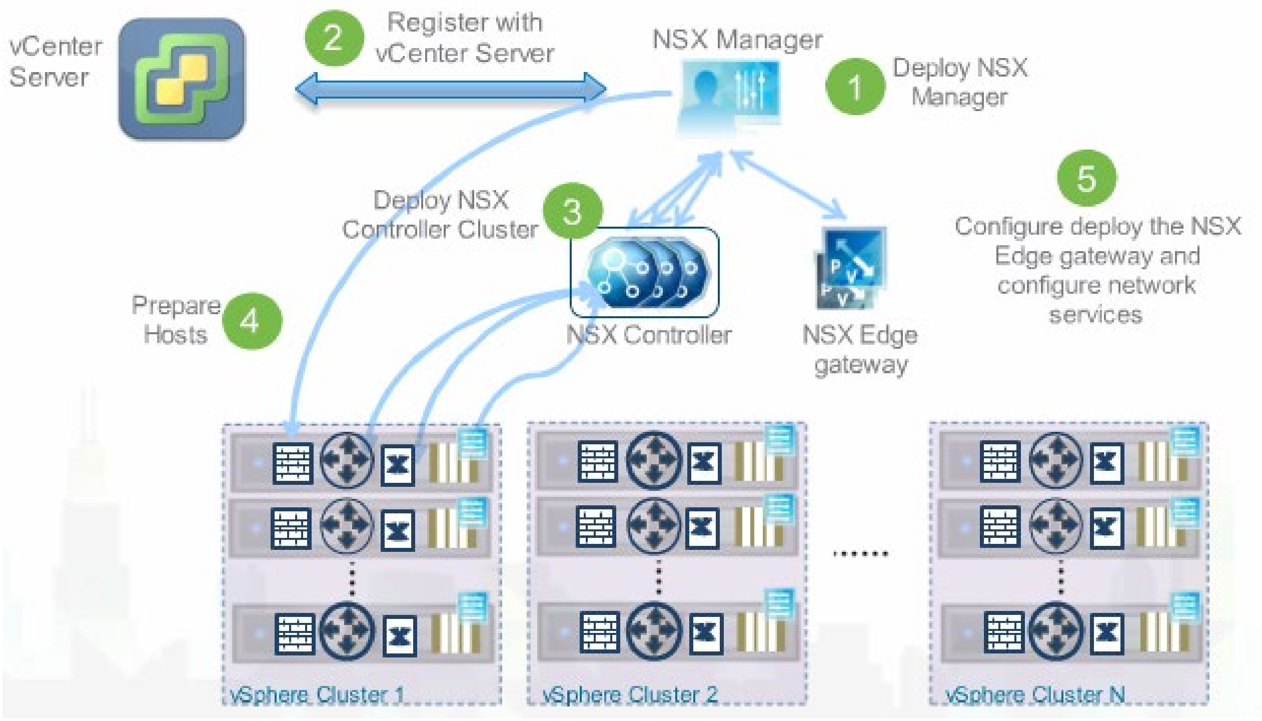
Organisations who have already invested in VMware infrastructure are at an obvious advantage. NSX data plane components are already embedded into the latest versions of vSphere at the hypervisor level, providing the base for distributed virtual switching and edge services along with L2 bridging to physical networks.

Control plane components are introduced on top, facilitating the use of logical networks and VMware vCentre is a prerequisite for the NSX management plane. At the top of the stack NSX integrates with the vRealize suite for cloud operations, automation and self-service.


Consumption Model
CMS
Management Plane
NSX Manager
vCenter Server
Message Bus Agent
Control Plane
NSX Logical Router Control virtual machine
NSX Controller
User World Agent
Data Plane
NSX vSwitch
VDS
ESXi
Hypervisor Kernel Modules
VXLAN
Distributed Logical Router
Firewall
NSX Edge Services Gateway
• Self Service Portal
• Cloud Management
• vRealize Automation
• Single point of configuration
• REST API and UI interface
• Manages Logical networks
• Run-time state
• Doesn't sit in the Data Path
• Control-Plane Protocol
• NSX vSwitch
• Distributed network edge
• Line Rate performance
• NSX Edge
• virtual machine form factor
• Data Plane for North South traffic
• Routing and Advanced services

Deployment

Deploying NSX can be straightforward with the right planning and design, and can be installed on top of any network hardware. Note the direct relationship between vCentre and NSX Manager.



To maximise the technology, the real focus and effort comes with tight integration into an environment, whether upgrading an existing one or planning a greenfield site. NSX is a powerful platform which can drive complexity when considering configuration and customisation, and associated elements and polices.

Summary

NSX is changing the face of network virtualisation and with benefits already being realised at the enterprise customer level, indications are that its adoption will continue to grow as organisations understand the benefits of network virtualisation.

A well-engineered physical network will always be an important part of the infrastructure, but virtualisation makes it even better by simplifying the configuration, making it more scalable and enabling rapid deployment of network services.

Businesses are exploring NSX and network virtualisation because they are able to achieve:

- Significant reduction in network provisioning time
- Greater operational efficiency through automation
- Improved network security within the data centre
- Increased flexibility and agility

The use cases for NSX are moving from 'presentation world' to the real world and most major innovations VMware are working on rely on NSX for the virtualisation of the network. With the rise of containers and isolated application environment, the micro-segmentation use case will become even more prevalent as it delivers a fundamentally more secure data centre.

SDN has also created an interesting dynamic for the SysAdmin. Does the virtualisation expert become a networking expert as well? Or does it fall into the network engineer's domain… we're already seeing a transition to the former, and a further evolution of IT support roles in general so it will be interesting to see how this develops.

Xtravirt are the experts in NSX solution design and integration and can help deliver an accelerated and non-disruptive SDN transformation for your organisation. To find out more about how we can work with you, contact us today.

About the author

Andy Hine joined Xtravirt in August 2015 as a Technical Pre-Sales Consultant. He has over 15 years' experience in IT across various industries and technologies. He has been involved in many transformation projects, architecting and enabling solutions in IT infrastructure and systems management, EUC/application delivery, virtualisation and cloud transition. Andy has a wide array of technical skills mainly focused on VMware, Citrix and Microsoft technologies.

About Xtravirt

Xtravirt is 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.

Our core business covers digital infrastructure, hybrid cloud, digital workspace and cybersecurity. Our services include advising strategy and direction, optimising and integrating technology and teams through to delivering end-to-end IT transformation programmes.