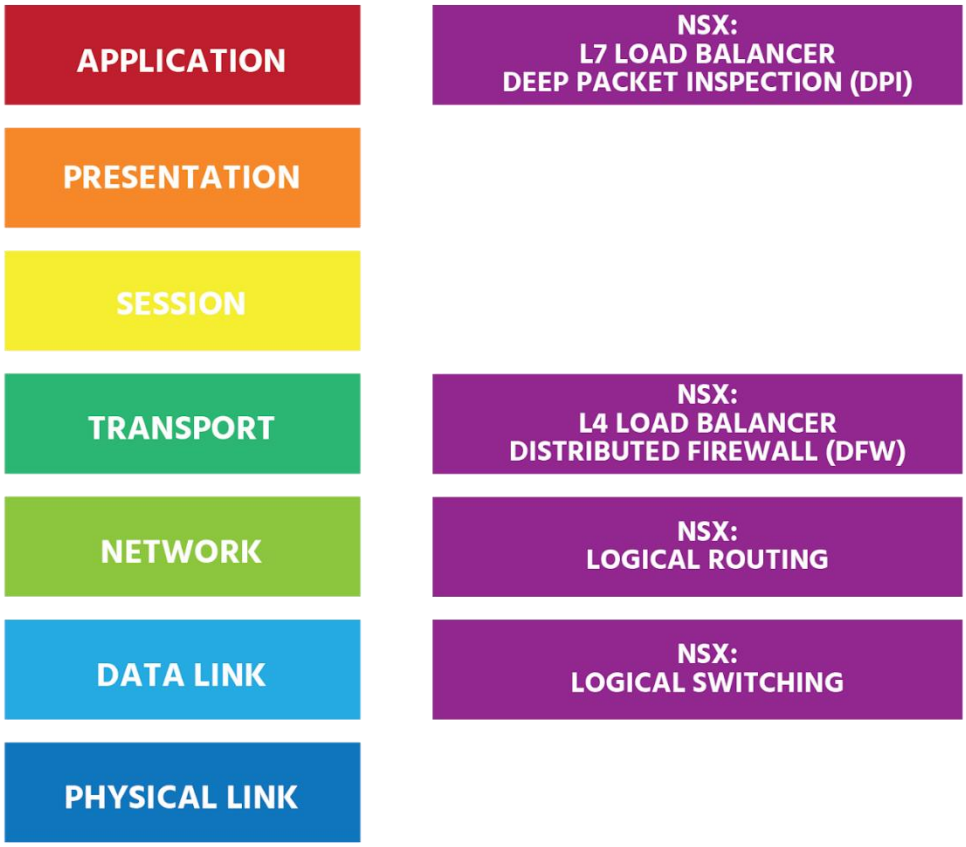
Module 5: The NSX Data Centre

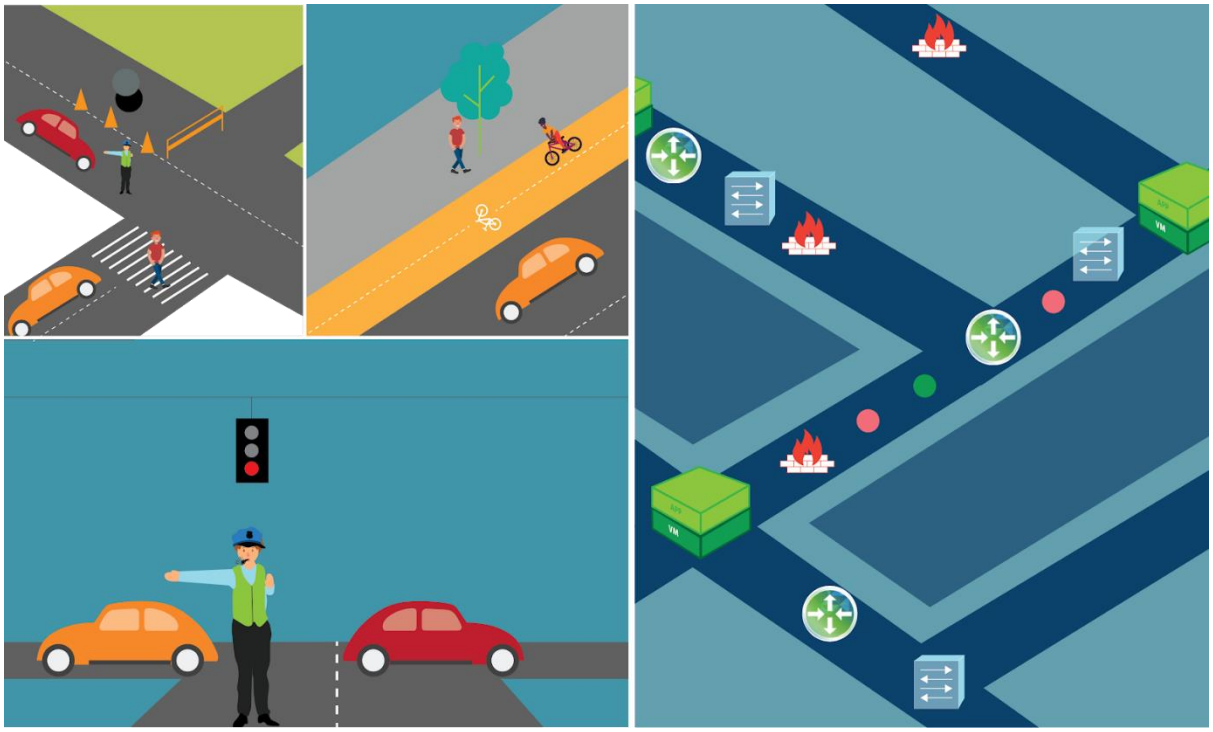
The NSX Data Center



In Information Technology (*IT*), the quest is always to do more with less, and for that you need a network that's secure enough to fortify you from threats, fast enough to meet your business needs, and agile enough to instantly accommodate your demands - while spending less time and money to get it all done.

The *NSX Data Center* – as part of a *software-defined data center* (SDDC) - achieves this. It's a totally new approach. It reproduces the whole network, whether the network is simple or complex, in software. Provisioning and managing networking functions (from firewalling, to switching, to routing, to load balancing) in software instead of hardware results in level security, speed, agility, and cost-efficiency that simply isn't possible with the traditional architecture.

For even greater control of your *SDDC*, *vRealize Network Insight* gives you a 360° view across virtual, physical, and multi-cloud environments to help you quickly troubleshoot connectivity issues.



For example, if two virtual machines are unable to talk to each other, or there are bottlenecks between two VMs, issues can be quickly pinpointed for rapid resolution. This 360° view also provides you with insights into applications' dependencies (that's all the programs they depend on to function properly), while you're planning application migration to a public cloud, a different data center, or a disaster recovery site.

Different areas of your network require different rules for security. *vRealize Network Insight* allows you to plan security for applications across private, public, and hybrid clouds. It helps accelerate micro-segmentation deployment by providing recommendations for *VMware NSX* firewall rules. *vRealize Network Insight* gives you a view of your entire NSX infrastructure with a powerful topology map that alerts you to potential issues and even provides recommendations for fixes.

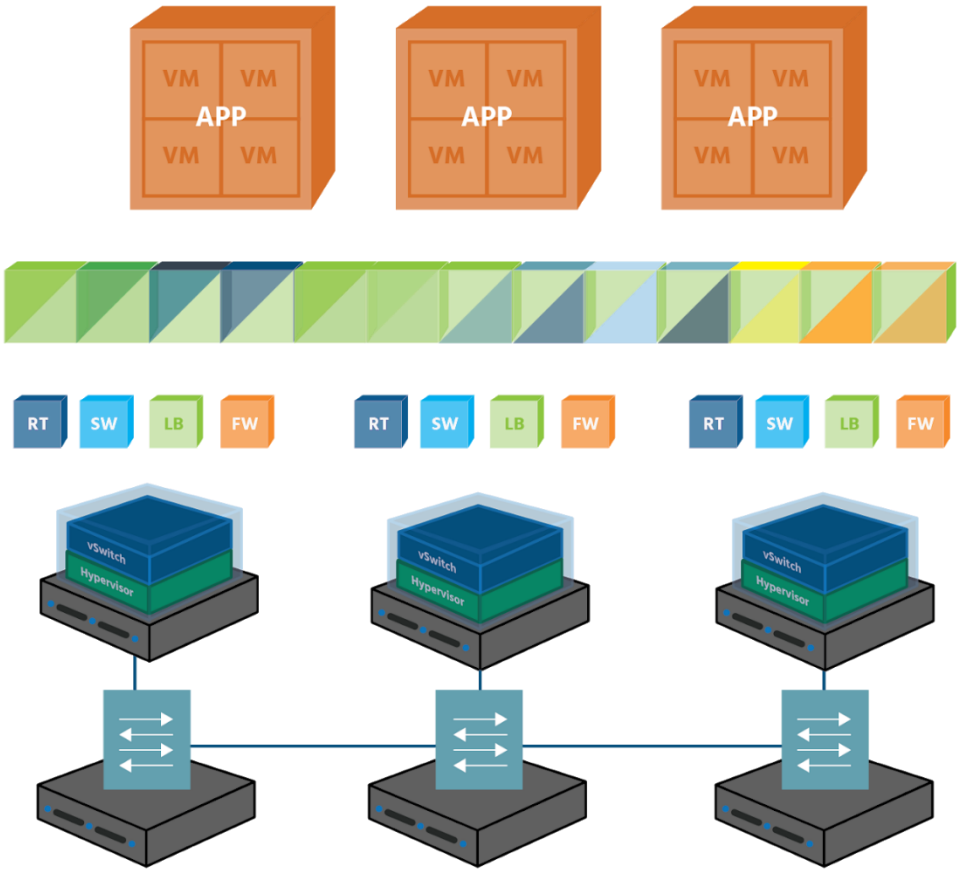
With so much control of your networking environment, all your teams will move faster and more safely.

NSX-V was first released in 2013 and met a real need in the market - within a few months three of America’s top five investment banks and several of the most respected enterprises around the world were using it. It went on to become the leading network virtualization platform and continues to serve the needs of its customers. However, times change. Not all applications run in VMs now. Containers and cloud-native apps are increasingly the norm. It was for this transformed environment that VMware developed NSX-T Data Center.

(The “T” stands for “Transformers”.) It has some common features with NSX-V, as we’ve seen. Both provide software-based network virtualization using software-based overlay technologies. Both provide distributed routing and firewalling. And both provide automation to increase agility. But unlike NSX-V, NSX-T is not tightly-integrated with vCenter. It works in all types of environments to connect all types of applications. It can support multiple hypervisors (ESXi and KVM); connect with a VM, a container, or a bare metal server (i.e., a physical server used by just one customer), on-premises or in a private cloud, public cloud, or multi-cloud environment; and integrate seamlessly with *Kubernetes, Docker, OpenStack, VMware Pivotal Container Service* (PKS), *Red Hat OpenShift, Pivotal Cloud Foundry, Amazon Web Service* (AWS), and *Microsoft Azure*.

VMware will continue to develop NSX-T Data Center to meet the networking and security needs of the future.

Bringing Network Virtualization to the SDDC



In a survey of its more than half-a-million customers, VMware found that 70% of respondents had virtualized over 75% of their IT infrastructure. However, only 12% had virtualized their networks, meaning that they weren’t yet

benefiting from the increased operational, time, and cost efficiencies to be gained from a fully software-defined data center.

VMware NSX is the industry leader for network virtualization. By abstracting the traditionally physical infrastructure of routers, switches, load balancers, and firewalls into a data center's virtualization layer, the data center becomes agile and responsive to business needs as they change. Virtual networks can be created, copied, moved, deleted, and restored quickly and easily, with no physical reconfigurations necessary.

With micro-segmentation (which we'll discuss later on in this course) threats are prevented from moving laterally, server to server, inside the data center. You can also tie security policies directly to an application and ensure that even as the application changes over time, it will maintain its protection.

Automation brings immediate gains in efficiency and innovation while enabling IT to keep up with the speed of business. The *NSX Data Center* uses standardized, pre-defined templates, to provision consistent networking and security, speeding up provisioning time from days or weeks to seconds.

Multiple users can share the same physical environment and cloud environment using virtual networks invisible to each other. So, everyone is working more efficiently than ever. With *NSX Data Center* for *Multi-cloud Networking*, you can replicate the networking and security configuration of your environment across multiple clouds and physical sites, ensuring continuous availability of resources and services. You can also seamlessly connect applications deployed anywhere, and extend your on-site network to the public cloud, moving applications back and forth as your needs change.

Key Components

NSX-T provides networks that support any application on any compute platform in any infrastructure. NSX-T networks provide connectivity, security, and availability, all through one set of management tools and all in software.

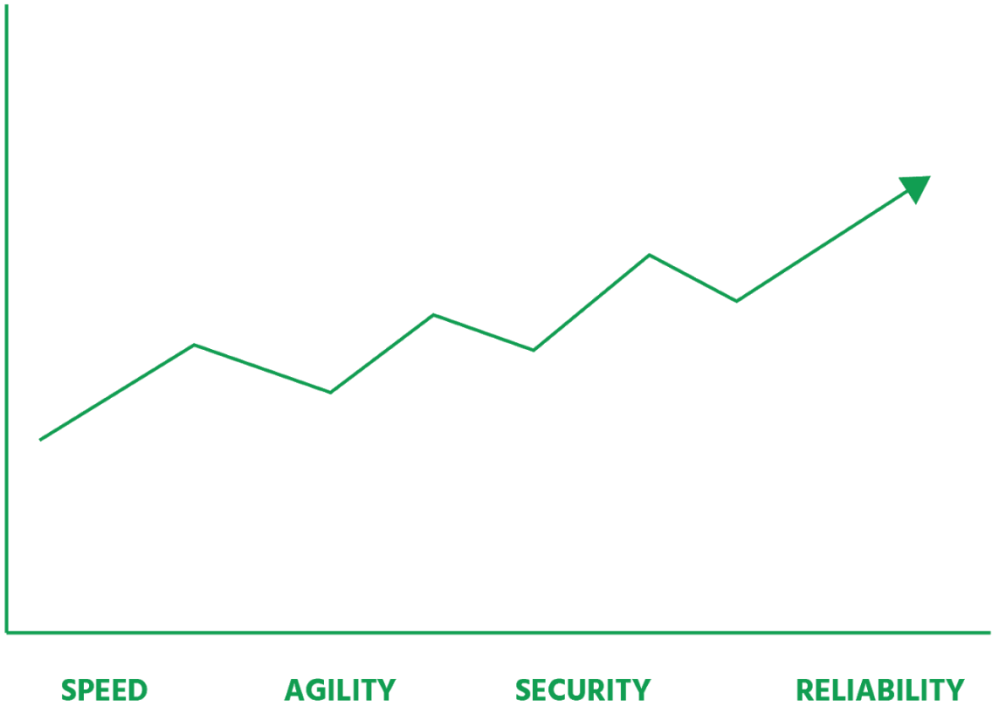
With NSX-V, the *NSX Manager* centralizes the management of a network and is available in the *vSphere Client*. (vSphere virtualizes and aggregates - i.e., gathers together - the underlying physical hardware resources across multiple systems and provides pools of virtual resources to the data center.) The *NSX Manager* is based on the Photon operating system - a Linux distribution developed by VMware and optimized for cloud-native applications, cloud platforms, and VMware infrastructure. The *NSX-T Manager*, on the other hand, runs on the Ubuntu operating system - a Linux distribution developed by Canonical and used on desktops and in data centers all over the world.

Administrators usually tie network virtualization to their cloud management platform, and NSX can be integrated with any cloud management platform through *Representational State Transfer* (REST) APIs. A REST API is a software architectural style that allows NSX objects such as logical routers and switches to be created, retrieved, changed/updated, and deleted. NSX-V can be configured through vSphere Client, through a command-line interface (CLI), and through a REST API.

Some of NSX Data Center's other key components include:

- *logical distributed* (i.e., spread out but connected) *switching* which allows you to reproduce the complete Layer 2 and Layer 3 functionality in a virtual environment, decoupled from the underlying physical hardware.
- *NSX Gateway*, a Layer 2 gateway that enables seamless connection to physical workloads and legacy VLANs.
- *logical routing* between logical switches which enables distributed routing between different virtual networks.
- *logical distributed firewalling* which allows you to create a distributed firewall that's integrated into the virtual networking layer, with security wrapped around each workload; application identification comes as standard, allowing you to identify and inspect network traffic, and allow or deny access as necessary; user-based firewalling also comes as standard, allowing you to create security policies aligned to users rather than to IP addresses that constantly change as users change devices/locations.
- a *logical load balancer* with SSL termination (which decrypts SSL-encrypted data).
- *logical VPN* for site-to-site and remote access VPNs in software.
- *service insertion* which enables you to apply third-party services to north-south traffic as well as east-west traffic that passes through a router.
- *multi-site, multi-cloud networking and security* which allow you to extend these technologies as widely as your current needs and future ambitions require.

Key Benefits



NSX Data Center helps organizations achieve the speed, agility, security, and reliability of the software-defined data center. It brings the benefits of compute virtualization to the whole data center, enabling entire networks to be created in software, and moved, copied, or deleted as easily as a virtual machine can be.

Every physical networking element and service in a traditional environment can be recreated in software – in seconds: logical switches, routers, firewalls, load balancers, and VPN, as needed.

It no longer takes weeks to provision today's complex networking and security services, because *NSX Data Center* does this in minutes. Automation (in which individual tasks are programmed to run by themselves) and orchestration (which is the coordination and management of many automated tasks) greatly reduce the amount of time-consuming manual configuration that administrators need to do, which in turn greatly reduces the amount of costly human error.

Because virtual machines in an *NSX Data Center* interact with each other through the vSwitch, the number of *east-west* (i.e., server to server) *hops* (or devices that data must pass through en route to its destination) is reduced. Network traffic flows are simplified.

The *NSX Data Center* uses **Equal-Cost Multi-Path** routing (*ECMP*) in which up to eight active *NSX Edge* appliances can be deployed at the same time and which increases the amount of data that can be sent from one point to another in a set amount of time (*the bandwidth*) for north-south communication. physical to logical (traffic from outside world to the data centre) ECMP means that NSX virtualized networks will keep on working even if multiple devices fail at the same time, giving NSX data centers high availability.

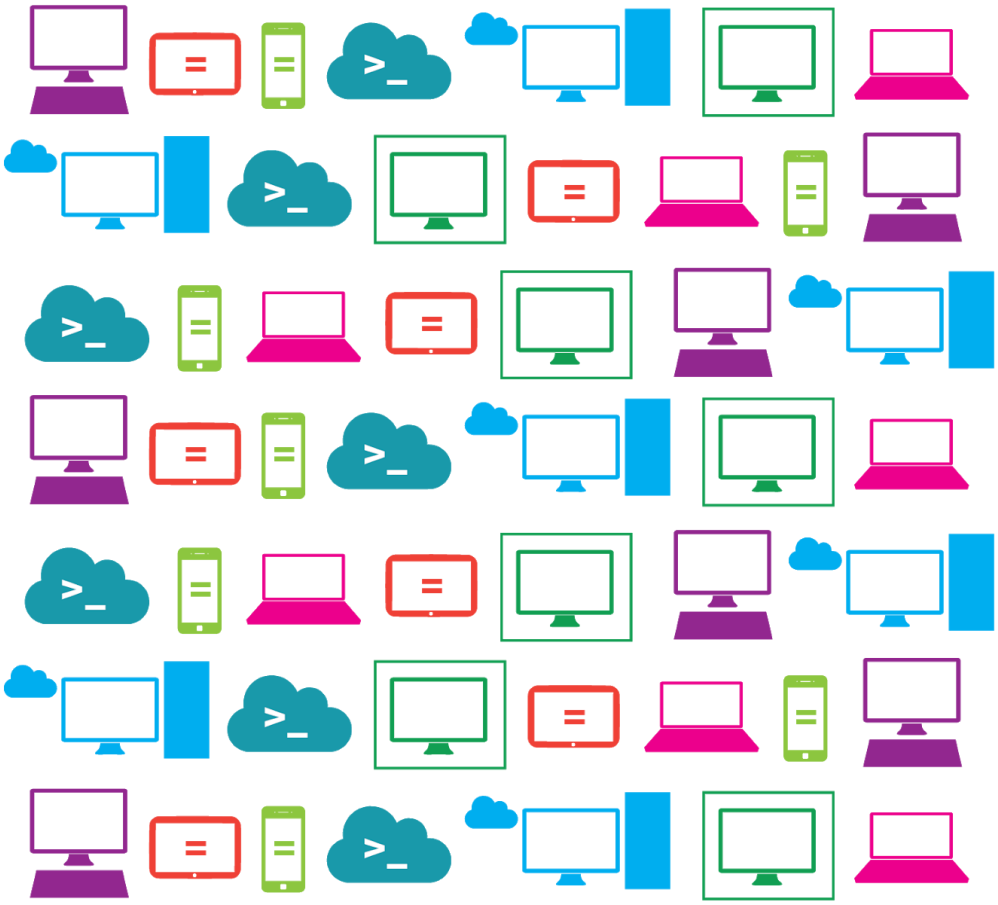
When the *NSX Data Center* is used with *vRealize Automation*, an NSX app isolation policy acts as a firewall to block all inbound and outbound traffic to and from workloads. Workloads can then communicate with each other but cannot connect outside the firewall. Threats can, therefore, be contained and data breaches (each one currently costing over $3.5m on average globally) can be reduced.

With security policies attached to the applications they're protecting, there's no longer a need to spend large amounts on additional hardware and software to firewall east-west traffic inside the data center.

Whereas in traditional infrastructures, new physical servers had to be bought to increase capacity, the *NSX Data Center* can bridge two or more network clusters to use any spare capacity that's already there. Existing server capacity is therefore used better, and money is saved. Further financial savings can be made in the underlying physical hardware that is still used to forward data (*the underlay*), as this can be off-the-shelf, industry-standard hardware. Expensive-to-buy and maintain vendor-specific hardware is no longer needed. And because the underlay has less to do, it should last longer; another cost-saving.

As discussed in section 5, *vRealize Network Insight* provides a 360° view of your entire NSX infrastructure. It is simple to use and makes it easy to access NSX activities and security events (records of security actions). In addition, *vRealize Network Insight* integrates with all major third-party network vendors.

Integrating with Existing Network Infrastructure



Administrators face persistent challenges as the demands placed on their networks by ubiquitous computing, the internet of things, voice over IP, and video over IP continue to grow. Capacity and security are two constant concerns; being able to monitor, manage, and troubleshoot multi-site networks (including different cloud environments) is another; the scalability of their infrastructures, compliance, advances in technology – the list goes on. Just keeping pace with these real and ever-present challenges can make the prospect of transitioning to a new networking model seem more daunting than it might actually be.

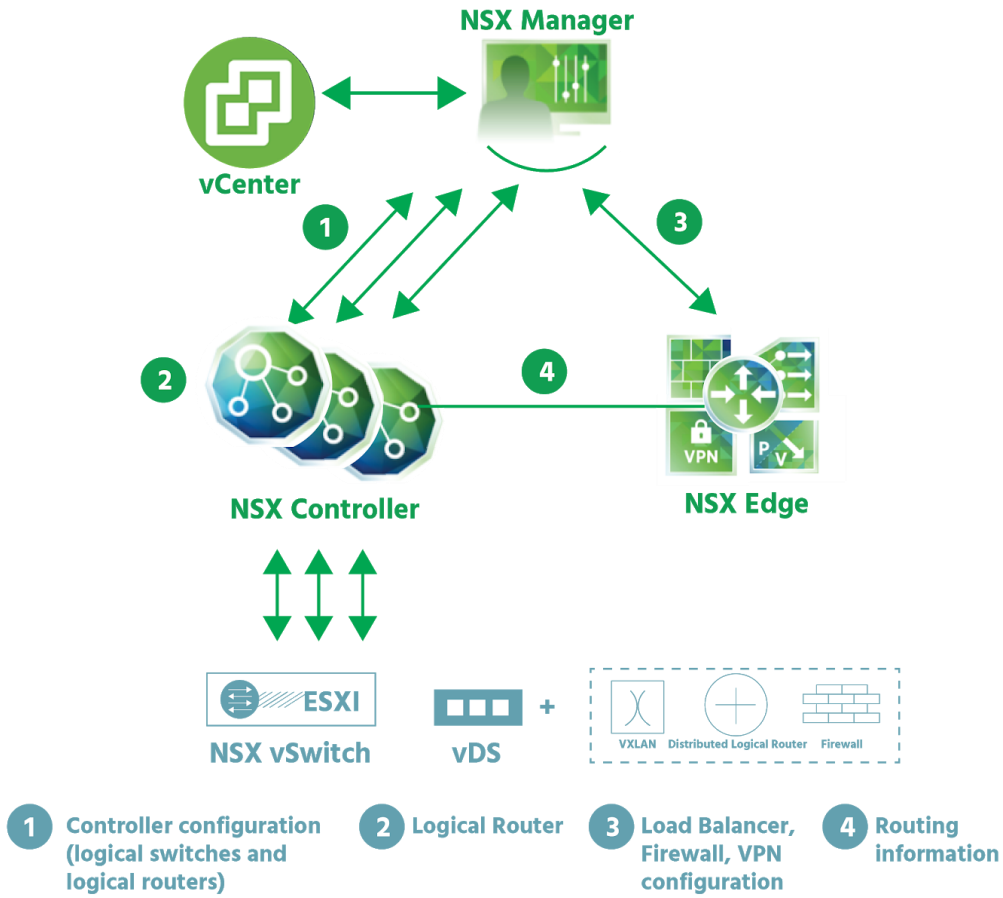
The *NSX Data Center* can be deployed without disruption to existing compute and networking infrastructure, applications, and security products because it works with them. It can be deployed over any existing network infrastructure and gives administrators the flexibility to virtualize as little or as much of their networks as they choose.

NSX provides networks that support any infrastructure, any compute platform, any application, any device, and any cloud.

The existing underlying physical network remains to handle packet forwarding but, once *NSX Data Center* is deployed, it barely needs to be touched and can, in fact, be streamlined. And if over time, parts of the physical network

need to be replaced, any off-the-shelf, industry-standard hardware can be purchased, providing even more flexibility.

NSX Architecture



NSX offers a complete suite of simplified logical networking elements and services, including logical switches, routers, firewalls, load balancers, VPN, monitoring, security, and quality of service. (*Quality of service* or QoS manages packet loss, transmission delay, and other issues on a network.) These services are provisioned in virtual networks through any cloud management platform using NSX APIs.

To existing workloads, virtual networks operate exactly as physical networks do – there's no difference. NSX distributes virtualized network and security services to each workload. Wherever workloads move, their services move with them.

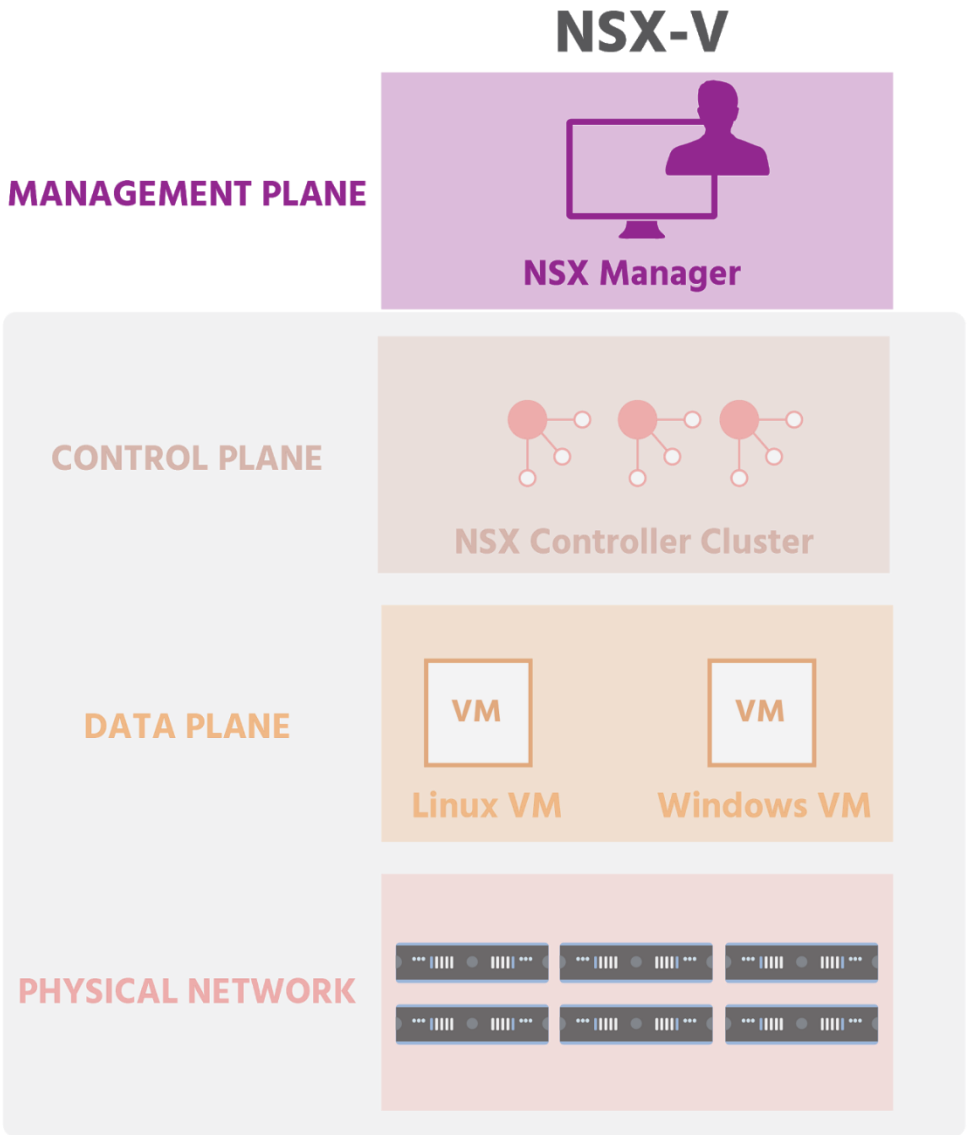
NSX architecture consists of a data plane, control plane, and management plane. Each plane consists of multiple components, responsible for platform management, traffic control, and service delivery. The architecture also includes the necessary components for integration with a cloud management platform.

We will look at each of the three planes next.

Management Plane

The NSX-V management plane is built by **NSX Manager**, the centralized network management component of NSX. *NSX Manager* provides configuration and orchestration of logical switching and routing, the distributed firewall, networking, Edge services, and security services.

NSX Manager is installed as a virtual appliance on an ESXi host in a vSphere environment. There is a one *NSX Manager* per *vCenter Server Appliance*. (vCenter Server Appliance is the central point for configuring, provisioning, and managing virtualized data centers.)



NSX Manager provides an overall view of a system. The single unified user interface allows you to manage both vSphere and NSX within the vSphere Client. (vSphere is the industry-leading virtualization and cloud platform and is

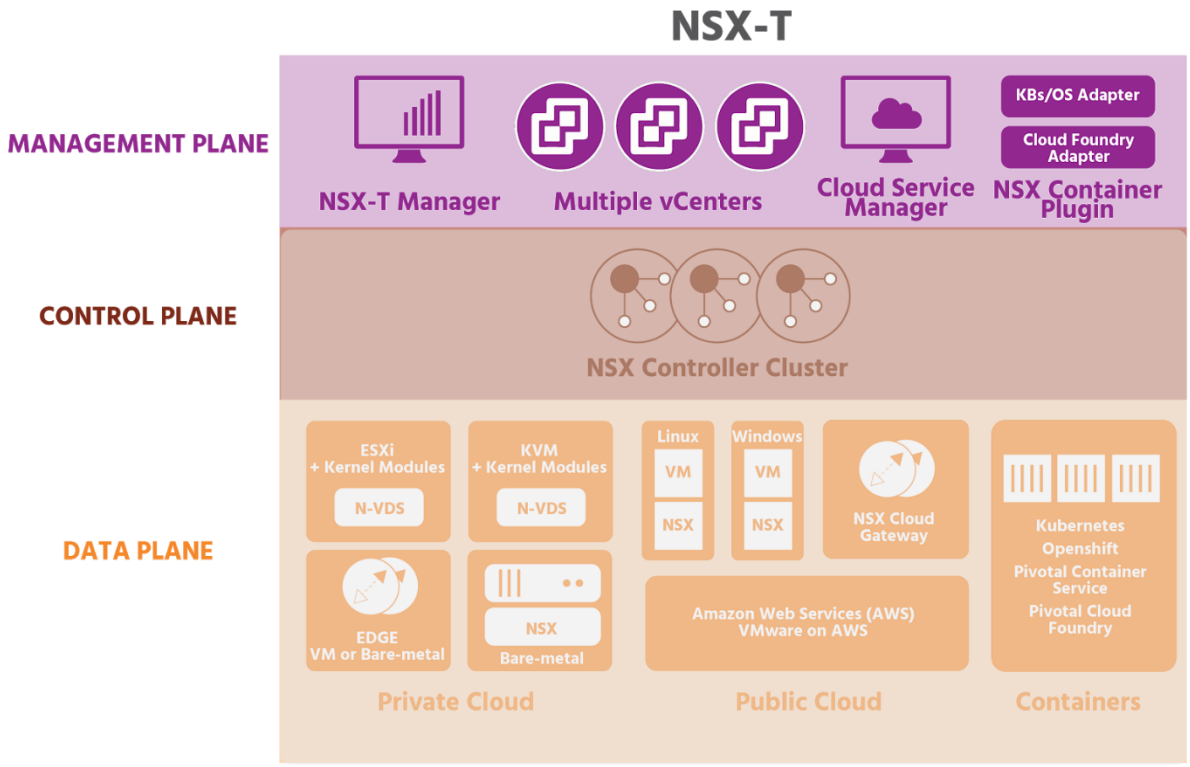
made up of the ESXi hypervisor, vCenter Server, and vSphere Client; with vSphere Client, a web browser can be used to connect to remote desktops and applications.) For NSX-V, a networking and security plug-in for the vCenter Server user interface (UI) enables administrators to configure and control NSX.

NSX Manager is not only able to orchestrate *built-in* Edge services and security services, but also those of third-party vendors.

If REST APIs need to be used (if, for example, an administrator wants to request something that isn't available via the graphical user interface – GUI – but needs to be requested directly from NSX; or if an administrator wants to use scripting to automate a task), this is done with *NSX Manager* and the administrator's REST client (software).

A few of the many VMware and third-party products that NSX integrates seamlessly with include:

- *VMware vRealize Automation* which streamlines the provisioning process and keeps networking and security services in sync with applications
- *VMware vRealize Log Insight* which provides real-time log management (a log is a record system processes, events, and messages)
- *VMware vRealize Operations Manager* which uses data collected from system resources to identify issues and either suggests corrective actions or offer helpful analytical tools
- *VMware Integrated OpenStack* which is VMware-supported OpenStack distribution that makes it easy to run an enterprise-grade OpenStack cloud on top of VMware infrastructure (OpenStack is a free and open-source cloud operating system)
- *VMware vRealize Network Insight* which gives users a micro-segmented view of their applications and a 360-degree view of their physical and virtual networks
- *Tufin Orchestration Suite for Firewall Management* which enables users to visualize and control their network security policies across all on-premise environments and cloud platforms

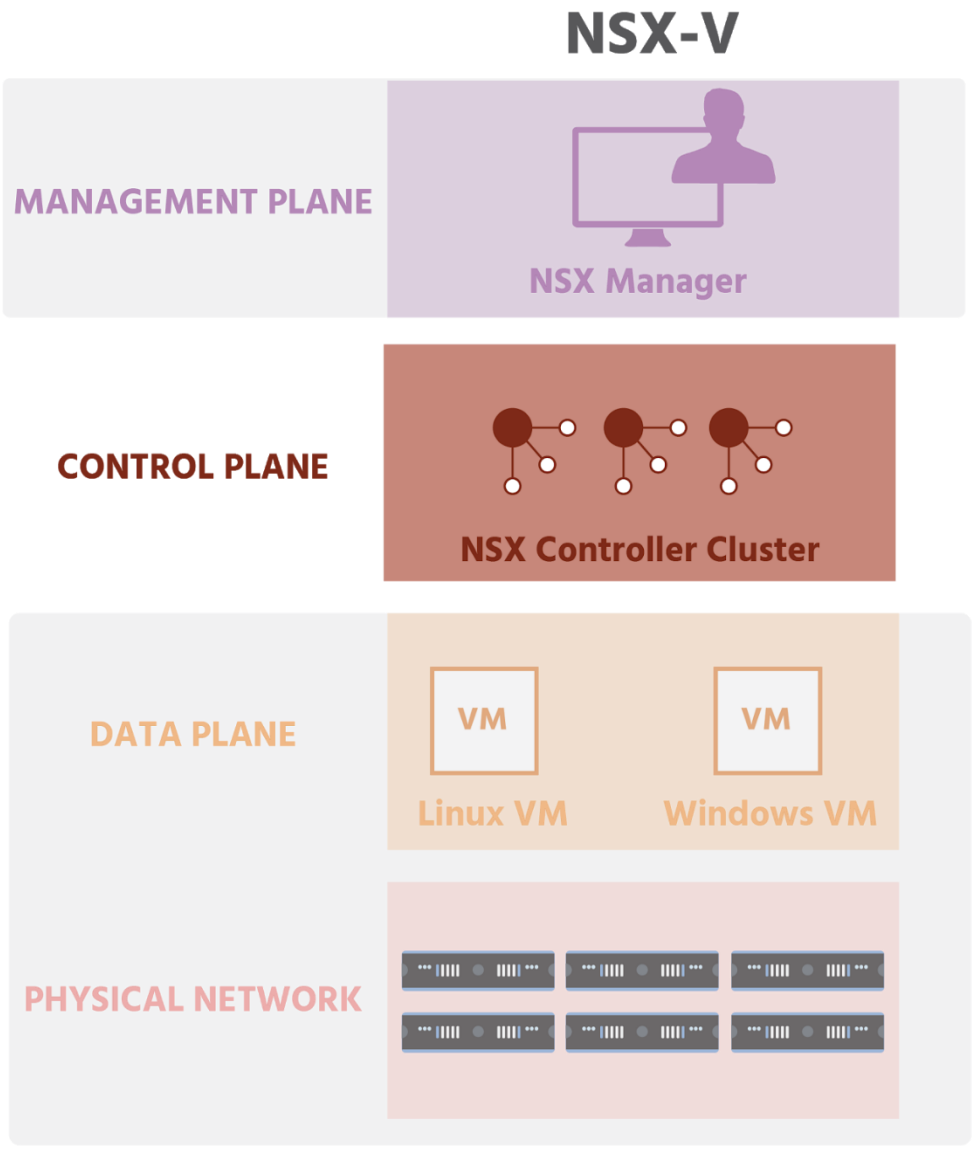


In a NSX-T Data Center, the management plane function and the central control plane function have been collapsed into a new management cluster to reduce the number of virtual appliances that need to be deployed and managed by the NSX administration. The NSX Manager appliance is available in three different sizes: a small appliance for lab or proof-of-concept deployments; a medium appliance for deployments to 64 hosts; and a large appliance for customers who deploy to a large-scale environment.

Control Plane

The control plane of NSX-V runs in the NSX Controller cluster. The *NSX Controller* serves as the central control point for all logical switches within a network, and maintains information about all hosts, logical switches, and distributed logical routers. Controllers distribute network information across all controllers in a cluster and are responsible for distributing network information to all the ESXi hosts. Controllers do not have any data plane traffic passing through them.

The controller cluster is responsible for managing the distributed switching and routing modules in the hypervisor.



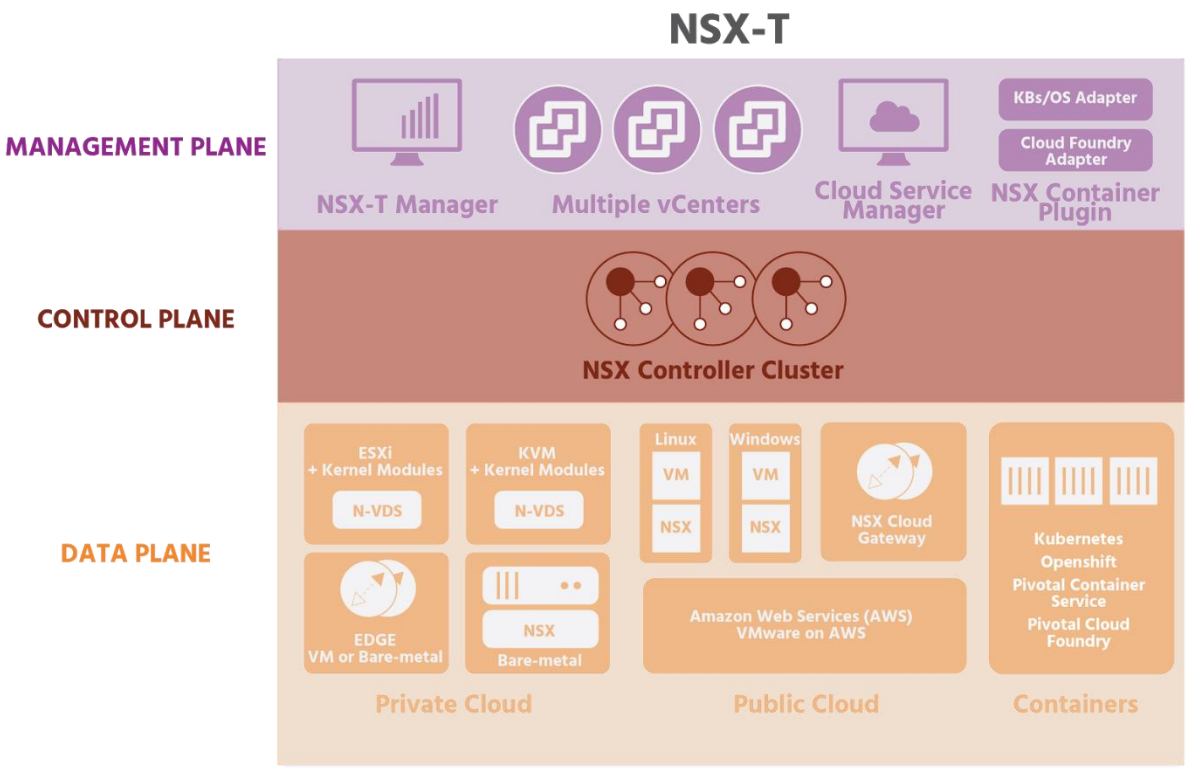
Network virtualization functions are distributed among the controllers. No matter the size of the *NSX Data Center* for vSphere deployment, a minimum of three *NSX Controller* nodes *must* be created in each NSX Controller cluster. In the event of a controller failure, the surviving controllers will assume the additional workload.

In NSX-T, whenever a *Distributed Logical Router (DLR)* is deployed, a *control VM* is automatically created. (With NSX-V, control VMs are optional - not created automatically - and are used for dynamic routing and Layer 2 bridging.) The control VM communicates with the NSX Controller cluster to ensure that the control plane has the most up-to-date routing table. The Controller cluster then programs the latest routing table on ESXi hosts through a *User World Agent (UWA)*. While the control VM does not itself route packets, it does make routing possible by the data plane:

- local forwarding within an ESXi host

- dynamic routing between ESXi hosts
- north-south routing provided by the Edge

UWAs pass virtual machine MAC addresses and IP addresses to *NSX Controllers*.

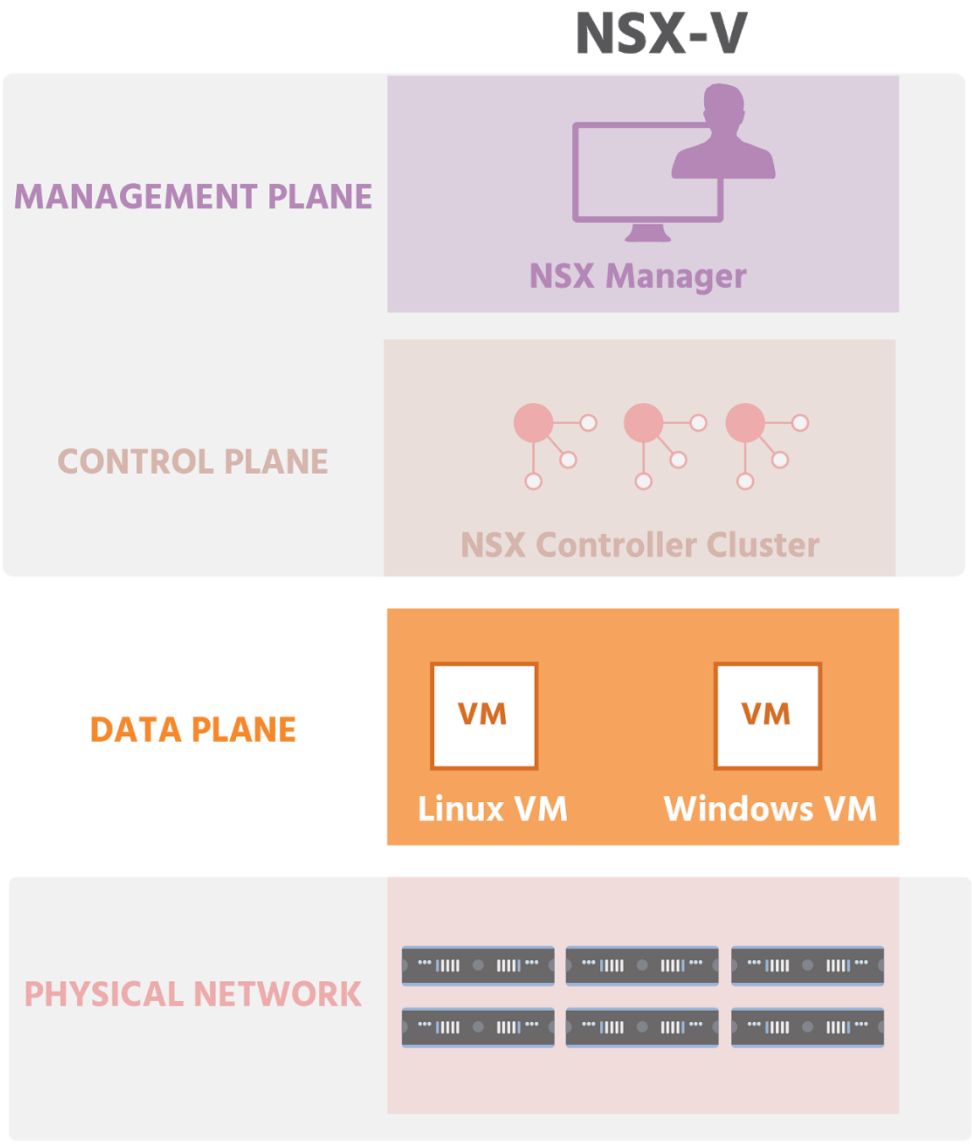


As mentioned in the last section, with NSX-T version 2.4, NSX Manager and NSX Controller have been combined.

Data Plane

The NSX data plane is where the actual network traffic flows. It consists of the NSX virtual switch, which is based on the **vSphere Distributed Switch** (*vDS*) with additional components to enable services. These add-on components include kernel modules that run within the hypervisor kernel, providing services including distributed routing, distributed firewall, and communication from the logical network to the physical network (e.g., overlay to VLAN bridging, either at Layer 2 as NSX bridging or at Layer 3 as NSX routing).

The *NSX vSwitch* abstracts the physical network and provides access-level switching (which connects end-user devices to the network) in the hypervisor. It is central to network virtualization because it enables logical networks that are independent of physical constructs.



Logical switching enables an extension of a Layer 2 segment and IP subnets anywhere in the network, independent of the physical network design. Routing between IP subnets can be done in software without traffic leaving the hypervisor. Logical routing is performed directly in the hypervisor kernel. The **Distributed Logical Router** (*DLR*) provides the best path for the east-west traffic that flows within the virtual infrastructure.

NSX security enforcement is done directly at the kernel and vNIC level and includes:

- *Distributed firewall* for east-west Layer 2 to Layer 4 traffic
- *Edge firewall* for perimeter protection of north-south traffic
- *SpoofGuard* for validation of IP/MAC identity.

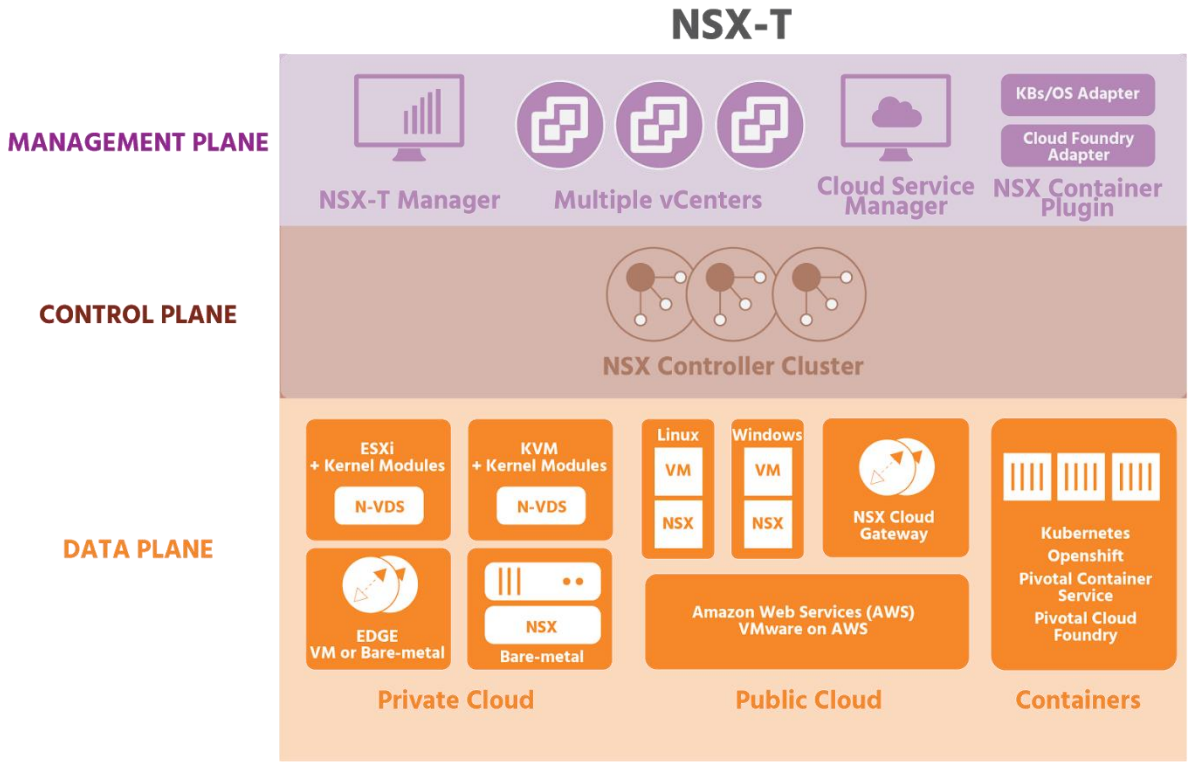
NSX also works well with security software from other vendors, including anti-virus/anti-malware/anti-bot products, file integrity monitoring, and vulnerability

management of guest VMs. It provides traffic management, monitoring, and troubleshooting within a virtual network.

NSX Edge provides a centralized point for seamless integration with the physical network infrastructure to handle communication with the external network routing (north-south communication), as well as perimeter firewall protection.

NSX supports NAT and DHCP, and can perform Layer 4 to Layer 7 logical load balancing (in two modes: inline and proxy mode, as discussed in section 4.6.2).

NSX VPN services (Layer 2 VPN, IPsec VPN, and SSL VPN) interconnect remote data centers and user access.



NSX can also be integrated with existing physical devices, including physical load balancers, firewalls, and monitoring devices.

Security Features

Traditional perimeter-centric firewall and intrusion detection and prevention systems cannot sufficiently protect the inside of a data center. There is limited (if any) isolation. Security controls within guest devices are not only vulnerable to attack but also drain resources and contribute to data congestion. Even if organizations are using the best-known security products, this sometimes only adds deployment and troubleshooting complexity to an already-complex job. Trying to get different products from different vendors to work together, especially without automation, can result in human error.

NSX provides unmatched security that's built directly into the data center. With it, organizations can streamline their networking and security operations, and automate the deployment of logical networks, firewalls, load balancers, and many other networking features. It is a complete platform for advanced networking and security and, as a result of using it, over 7,500 businesses – 82% of the Fortune 100 - are deploying networking faster and adapting to changes more easily.

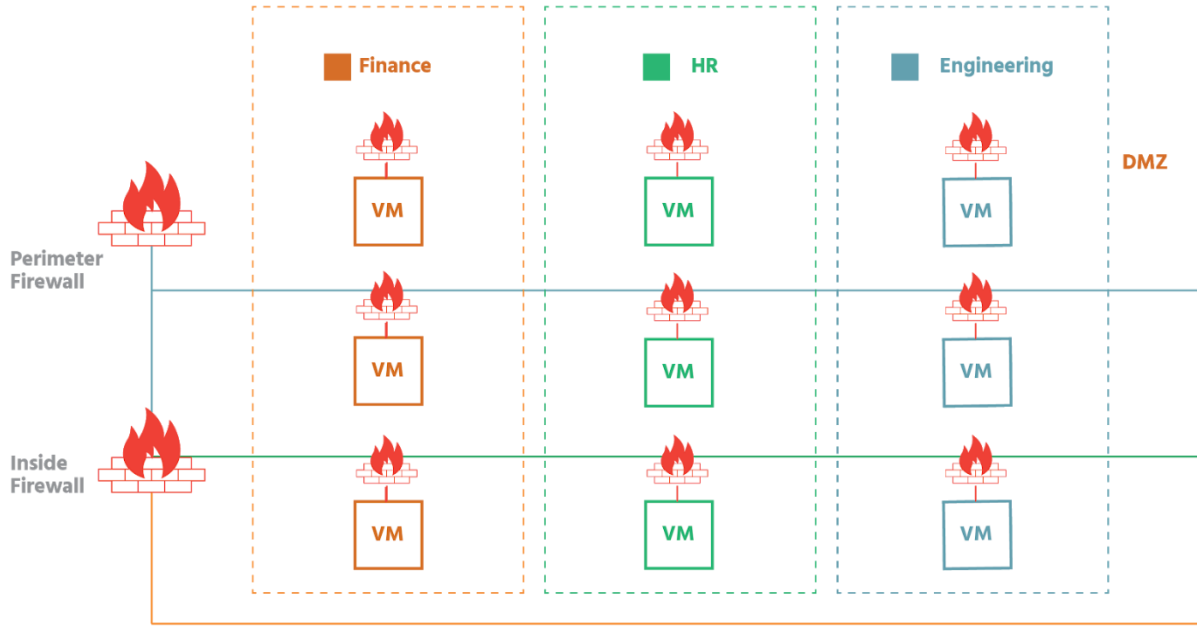
NSX embeds security functions directly into the hypervisor, providing micro-segmentation and automated, most-finely detailed (*granular*) security for every individual virtual desktop or device. This prevents threats from spreading in a data center, enabling a fundamentally more secure environment. NSX enables security policies to travel with specific workloads, wherever they are in the network and whenever they move.

Because virtual networks are isolated by default – isolated from each other and from the physical network that is their underlay – data centers deploying them are by definition, more secure.

A network will also include what's known as a **Demilitarized Zone** (*DMZ*) or *screened subnet*. This is a physical or logical sub-network of the main network that's positioned between external networks (e.g., the internet) and the main network. External networks can only connect with what is in the DMZ (such as web servers, email servers, file transfer protocol servers, and VOIP servers). The DMZ itself has limited access to the main network, which is protected behind one or more firewalls. The idea is that a hacker attack will not be able to penetrate into the main network, but will be contained within the DMZ. NSX can provide a logical DMZ anywhere in the data center, and, being software, it can be as large or as small as needed – from a single app to the whole data center.

NSX works seamlessly with third-party products, meaning that organizations can continue to use their preferred network security products without increasing the risks associated with manual configuration without automation.

Micro-Segmentation



Network traffic patterns have shifted drastically in recent years from mainly north-south (traveling from *outside* the data center perimeter to a server inside and then back) to east-west (traveling laterally between servers *inside* the data center perimeter). East-west traffic is in fact now thought to account for up to 80% of all network traffic. This significantly increased lateral traffic often

never passes through firewall controls. The need for *zero trust* has, therefore, never been greater. Zero-trust is an approach to network security (introduced by the technology market research company, Forrester, in 2010) that allows no traffic to move in within or in and out of a data center without first having its identity strictly verified based on user and location.

Network security teams have been trying to achieve the level of east-west security that micro-segmentation provides for years. The problem has been that implementing micro-segmentation on a large enough scale has been impossible. Even if a security team was somehow able to afford enough firewalls to inspect all east-west traffic, there's no way the team would be able to keep up with the rule management as new workloads were created, moved, and retired. And even with host-based firewalls running on the operating system of individual virtual machines (as has been popular over the last few years), determined hackers have simply disabled those firewalls, leaving the whole network exposed.

With NSX, the distributed firewall runs inside the kernel of the ESXi host- not in the operating system (OS). Micro-segmentation further simplifies network security. At its most basic, micro-segmentation is the ability to segment elements of a system into extremely granular components. The value of this lies in the fact that, once a network is segmented, security policies can easily be applied, whether an administrator wants to target a cluster of servers or a single VM.

To micro-segment a network, an administrator first creates logical groups called **security groups**. Security groups are containers that can contain multiple object types, including VMs, logical switches, vNICs, and **IPsets**. (*IPsets* store IP addresses, MAC addresses, and port numbers, among other things). Security tags (which are labels that can be attached to a VM), VM names and logical switch names can be used to add objects to security groups. For example, all VMs with the security tag *web* would automatically be added to a specific security group for web servers. Once the security groups have been created, the administrator creates the necessary security policies. The security policies are then applied to the appropriate security groups.

Each VM can now be on its own perimeter – have its own firewall. The security policies defined for it will go with it wherever and whenever it moves. Its security is no longer dependent on an OS-based firewall that could be disabled, making the VM the launch-point for a system-wide attack. Neither is the VM solely reliant on a physical firewall for its protection, in which scenario traffic leaves the VM, travels to the firewall for inspection, and is then either stopped or allowed to flow depending on the policy-settings. With the firewall now running in the kernel of the ESXi host, when VM1 wants to send data to VM2, the data is inspected when it reaches the vNIC of VM2.

Virtual networks are isolated by default- from each other and from the underlying physical network- and this provides an immediate security boost

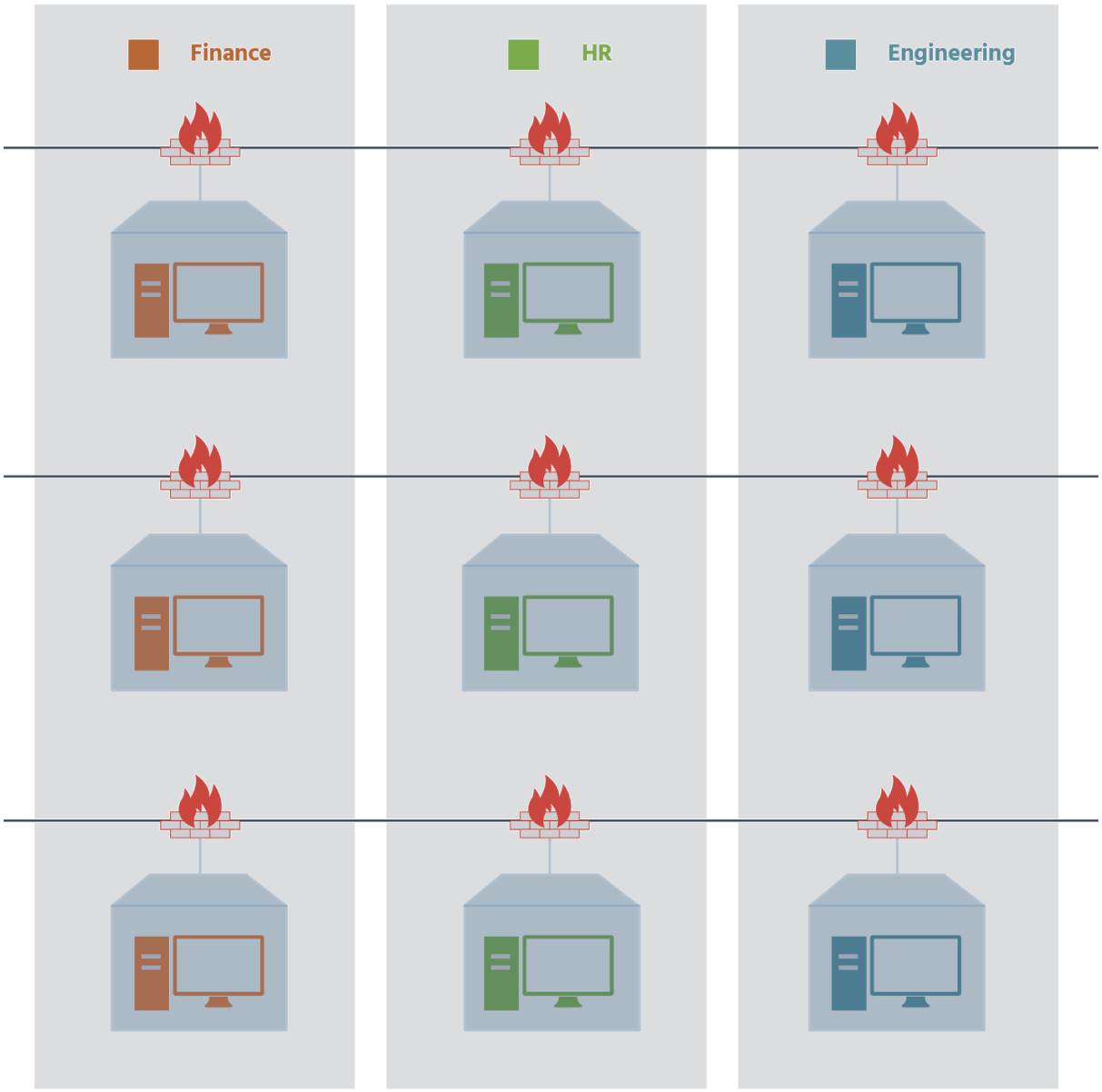
since a problem with one virtual network is contained to that one network. It will not spread.

Attackers can modify IP addresses to gain access to networks. NSX policies go beyond using IP addresses, taking into consideration the VM, the virtual network, the operating system, and more- streamlining configuration and reducing errors at the same time.

As mentioned in the last section, NSX works seamlessly with the best known security products. Administrators can, therefore, continue using their existing security products from vendors such as *Palo Alto Networks*, *Trend Micro*, *Symantec*, *McAfee*, and *Rapid 7*. On NSX, these security products use security tags to share security information in order to adapt to changing security conditions.

With the increasing adoption of the software-defined data center and network virtualization with NSX, micro-segmentation has become both operationally possible and economically practical for businesses. Administrators can directly target lateral east-west traffic traveling between VMs inside a data center. This makes NSX ideal for securing intra-data center network traffic, for fully isolating different networks (for example, for highly sensitive workloads) and for simplifying networks that would otherwise require complex access policies.

Secure End-User



Many enterprises have deployed *Virtual Desktop Infrastructure* (VDI) to take advantage of virtualization technologies beyond the data center. VDI is the technology that's used to provide and manage virtual desktops. VDI hosts desktop environments on a centralized server, and users connected to the network can access these virtual desktops from anywhere and any device.

Unfortunately managing groups of virtual desktop users is often a complicated process involving multiple teams. This is particularly complex in organizations with different user groups, each group having its own level of access to various resources.

NSX simplifies VDI by providing security based on logical groups of users or departments. This means that organizations are able to speed the deployment

of virtual desktop environments and use their resources more efficiently. Security is no longer constrained or defined by the network topology.

NSX micro-segmentation integrates network and security with VDI management, allowing for the creation of a single set of policies for as many different VDI users as necessary. Micro-segmentation of user environments also means that NSX is able to secure traffic between virtual desktops and adjacent workloads – a risk that many organizations are unaware of. With NSX, if one end-user's virtual desktop is attacked, the breach can easily be contained to just that user.

The automated application of network and security policies, and the fact that these policies seamlessly integrate with anti-virus and next-generation firewall vendors further simplify VDI for administrators.

The net value of this fundamental shift in networking and security is that businesses are able to provide a dramatically more secure infrastructure and do it in a way that's significantly cheaper than traditional approaches (at ⅓ of the cost), and much simpler to provide.

Virtual networking components

Section 4.1 | Section 4.2 | Section 4.3 | Section 4.6 | Section 4.6.1 | Section 4.7 | Section 4.7.1