LEARNING MADE EASY

2nd VMware Special Edition

Network Virtualization

for dummies®
A Wiley Brand

Seeing why you need to virtualize your network

Understanding how it works and getting started

Brought to you by vmware®

Jonathan Morin
Shinie Shaw

About VMware

VMware software powers the world's complex digital infrastructure. The company's compute, cloud, mobility, networking and security offerings provide a dynamic, consistent digital foundation to deliver the apps that power business innovation. VMware is streamlining the journey to digital business for more than 500,000 customers globally, aided by an ecosystem of 75,000 partners, by unlocking value from today's technologies while enabling the integration of tomorrow's. With VMware, organizations are empowered to flex and harness new technology quickly, without disrupting operations or introducing risk. This year, VMware celebrates 20 years of breakthrough innovation benefiting business and society.

To learn more, visit **www.vmware.com**.

Network Virtualization

2nd VMware Special Edition

by Jonathan Morin and Shinie Shaw

for dummies®
A Wiley Brand

Network Virtualization For Dummies®, 2nd VMware Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-55049-5 (pbk); ISBN 978-1-119-55054-9 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact Branded Rights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Development Editor: Becky Whitney
Project Editor: Elizabeth Kuball
Acquisitions Editor: Katie Mohr
Editorial Manager: Rev Mengle
Business Development Representative: Karen Hattan
Production Editor: Magesh Elangovan

Table of Contents

Introduction

Welcome to *Network Virtualization For Dummies*, your guide to a new and greatly improved approach to networking.

Before we get to the heart of the matter of network virtualization, let us briefly describe some topics that we cover within these pages. All the following requirements build the case for moving out of the hardwired network past and into the flexible world of network virtualization, which we describe in depth in Chapter 1:

- The network needs to move as fast as the business.
- Network security needs to move faster than cybercriminals do.
- Applications need the flexibility to run anywhere.

So, how do you get there? The first step is to immerse yourself in the concepts of this new approach to networking. That's what this book is all about.

About This Book

Don't let the small footprint fool you. This book is loaded with information that can help you understand and capitalize on network virtualization. In plain and simple language, we explain what network virtualization is, why it's such a hot topic, how you can get started, and steps you can take to get the best bang for your IT buck.

Foolish Assumptions

In writing this book, we've made some assumptions about you. We assume that

- You work in IT, cloud, application pipelines, or a related role that involves some level of networking.
- You're familiar with network terminology.
- You understand the concept of virtualization.

Icons Used in This Book

To make it even easier to navigate to the most useful information, these icons highlight key text:

REMEMBER

Take careful note of these key "takeaway" points.

TECHNICAL STUFF

Read these optional passages if you crave a more technical explanation.

TIP

Follow the target for tips that can save you time and effort.

Where to Go from Here

The book is written as a reference guide, so you can read it from cover to cover or jump straight to the topics you're most interested in. Whichever way you choose, you can't go wrong. Both paths lead to the same outcome: a better understanding of network virtualization and how it can help you increase security, agility, and multi-cloud flexibility.

IN THIS CHAPTER

- Exploring today's networking challenges
- Building the case for network virtualization
- Introducing the virtual cloud network

Chapter 1
The Next Evolution of Networking: The Rise of the Virtual Cloud Network

Why should you care about network virtualization? That question has more than a single answer. This chapter explores several challenges today that point to a single overarching need: Networking and security must be delivered in software. Here's why:

- To stay competitive, businesses need the agility of the cloud.
- Legacy network architectures limit business agility, leave security threats unchecked, and drive up costs.
- Dedicated hardware for each network function prohibits a different approach.

Network virtualization is rewriting the rules for the way services are delivered, from the software-defined data center (SDDC), to

the cloud, to the edge. This approach moves networks from static, inflexible, and inefficient to dynamic, agile, and optimized.

In this new world, virtualization enables the intelligence of the infrastructure to move from hardware to software. With the SDDC, data center infrastructure elements — including compute, networking, and storage — are virtualized and grouped into pools of resources. These resources can then be automatically deployed, with little or no human involvement. Everything is flexible, automated, and controlled by software. The virtual cloud network extends these concepts beyond the data center, to wherever applications and data reside.

With network virtualization enabling the SDDC, you can forget about spending days or weeks provisioning the infrastructure to support a new application. You can now deploy or update apps in minutes, for rapid time to value. This book has a particular focus on how network virtualization enables the SDDC, while also touching on how it lays the foundation for the virtual cloud network — a network model that extends network virtualization across clouds, across apps, across endpoints.

According to RightScale's "2018 State of the Cloud" report, 81 percent of enterprises are expected to have a multi-cloud strategy, with organizations leveraging five clouds on average. In order to realize this strategy, a software-defined approach is essential. It's really a much-needed framework for greater agility and more responsive service delivery from IT operations and development, all at a lower cost. It's the key to getting a handle on our multi-cloud future.

The Business Needs Speed

The chapter opener presents all the good news about network virtualization. Here's the catch: Network architectures rooted in hardware can't match the speed and agility of the SDDC.

Organizations of all sizes are experiencing a rapid increase in the pace of change. Everything needs to be done yesterday — new innovations and feature delivery, competitive responses, projects critical to the organization. This new reality has big implications for the network.

When a business wants to wow its customers with a new app, roll out a promotion, or take a new route to market, it needs the supporting IT services right away — not in weeks or even days. In today's world, you either go for it or you miss out. We're in the era of the incredible shrinking window of opportunity.

When the business turns to the IT organization for essential services, it wants to hear, "We'll get it done. We'll have it up and running right away." And increasingly, the business wants to not even need to ask IT.

Security Requirements Are Rising

Long ago, a young Bob Dylan advised the world, "You don't need a weatherman to know which way the wind blows." Today, you could say pretty much the same thing about network security. In today's enterprises, a roaring wind is blowing and serving as a security wakeup call.

Everyone knows we need to do more to avoid costly breaches that put sensitive information into the hands of cybercriminals. No company is immune to the threat. Just consider some of the headline-grabbing security breaches of the past few years — breaches that have brought corporate giants to their knees. Major brands, from healthcare and investment banking to retail and entertainment, have been tarnished after letting down their customers. All companies are now caught up in the same costly battle to defend critical data.

It's like one big war game. A company fortifies its data center with a tough new firewall and the cybercriminals slip in through a previously unknown back door — like a simple vulnerability in a client system — and run wild in the data center. The traditional strategy of defending the perimeter needs to be updated to include much more protection inside the data center.

Consider these research-driven insights:

- According to CSIS's 2018 report, "Economic Impact of Cybercrime — No Slowing Down," security losses are increasing year over year despite year-over-year increases in security spending.

» In a Gartner press release from August 2017, Sid Deshpande, principal research analyst at Gartner, said ". . . improving security is not about spending on new technologies. As seen in the recent spate of global incidents, doing the basics right has never been more important. Organizations can improve their security posture significantly just by addressing basic security and risk related hygiene elements like . . . internal network segmentation. . . ."

Observations like these underline the need for transforming the network through virtualization with built-in security.

Apps and Data Are in Multiple Clouds

There is no longer a simple answer for where apps are running and where their data resides. For many organizations, some apps start in the cloud, where some developers begin to code and test. Many also find that certain apps are best run in the private data center, both for the cost efficiencies and the private control. Many other organizations still have moved apps in either direction — from the private data center to the public cloud to delegate management, and from the public cloud to the private data center to reign in public-cloud costs or to take advantage of new private-cloud consumption models. Today, organizations realize that they need to rely on multiple environments.

The rise of server virtualization has made a lot of great things possible around application mobility, but there has been a catch: the network. It's like a hitch in your giddyup, to borrow some words from the cowboys of old. The network configuration is tied to hardware, so even if apps can move with relative ease, the hardwired networking connections hold them back.

Networking services tend to be very different from one data center or cloud to another. That means you need a lot of customization to make your apps work in different network environments. That's a major barrier to app mobility — and another argument for using virtualization to transform the network.

Network Architectures Rooted in Hardware Can't Keep Up with the SDDC

The SDDC is the most agile and responsive architecture for the modern data center. It's achieved by moving intelligence into software for *all* infrastructure elements. So, let's take stock of where things are today:

- Most data centers now leverage server virtualization for the best compute efficiency. *Check!*
- Many data centers now optimize their storage environments through virtualization. *Check!*
- Organizations have virtualized their network environments within the data center and across clouds. *A lot of progress has been made! But the potential to do more remains enormous.*

Though businesses are capitalizing on server and storage virtualization, they're still challenged by legacy network infrastructure that revolves around hardware-centric, manually provisioned approaches that have been around since the first generation of data centers.

In the following sections, we walk through some of the specific challenges of legacy architectures.

Physical network provisioning is slow in nature

Although some network provisioning processes can be scripted — and certain software-defined networking (SDN) models promise to make this a reality — with hardware-based systems, there is no automatic linkage to compute or storage virtualization. As a result, there is no way to automatically provision networking when the associated compute and storage is created, moved, snapshotted, deleted, or cloned. So, network provisioning remains slow, despite the use of automated tools.

All the while, the thing that matters the most to the business — getting new apps ready for action — is subject to frequent delays caused by the slow, error-prone, manual processes used to provision network services.

This is all rather ironic when you take a step back and consider the bigger picture: The limitations of legacy networks tie today's dynamic virtual world back to inflexible, dedicated hardware. Server and storage infrastructure that should be rapidly repurposed must wait for the network to catch up. Provisioning then becomes one big hurry-up-and-wait game.

Workload placement and mobility are limited

In today's fast-moving business environments, apps need to have legs. They need to move freely from one place to another. This might mean replication to an offsite backup-and-recovery data center, movement from one part of the corporate data center to another, or migration into and out of a cloud environment.

Server and storage virtualization makes this kind of mobility possible. But you have to be aware of another problem: the network. When it comes to app mobility, today's hardwired network silos rob apps of their running shoes. Workloads, even those in virtual machines, are tethered to physical network hardware and topologies. To complicate matters, different data centers have different approaches to networking services, so it can take a lot of heavy lifting to configure an app running in data center A for optimal performance in data center B.

All of this limits workload placement and app mobility and makes change not just difficult but risky. It's always easiest — and safest — to simply leave things just the way they are.

The current hardware-centric approach to networking restricts workload mobility to individual physical subnets and availability zones. To reach available compute resources in the data center, your network operators may be forced to perform box-by-box configuration of switching, routing, firewall rules, load-balancing services, and so on. This process is not only slow and complex but also one that will eventually reach scalability limits, either on the ternary content-addressable memory (TCAM) limitations of how many MAC and IP addresses the systems can retain, or on the architectural limitations of constructs like virtual local area networks (VLANs), which are still too often used as a segmentation mechanism despite the work-arounds and the 4,096 scale limitation.

Hardware limitations and lock-ins breed complexity and rigidity

The current closed black-box approach to networking — with custom operating systems, application-specific integrated circuits (ASICs), command-line interfaces (CLIs), and dedicated management software — complicates operations and limits agility. This old approach doesn't consider the dynamic nature of today's applications, and it locks you in — and not just with the vendor. It locks you into the complexities of your current network architecture, limiting your IT team's ability to adapt and innovate, which in turn puts the same limits on the business itself, because the business can move no faster than IT.

According to Gartner's 2018 "Look Beyond Network Vendors for Network Innovation" report, Gartner is seeing that as its clients are going through digital transformation, their network teams "must deliver data center network infrastructure rapidly and on-demand." Moreover, Gartner is seeing that the data center network is one of the biggest challenges for its clients (based on more than 3,000 inquiries and audience polling in 2017).

Here are some rather telling findings from the same report:

- It is common for data center network requests to take days to fulfill.
- The number of active ports supported per local area network (LAN) full-time equivalent (FTE) has actually gotten less efficient over time, by more than 10 percent — from 3,412 ports per FTE in 2013 to only 2,933 ports per FTE in 2016.

Configuration processes are manual, slow, and error-prone

On a day-to-day basis, physical networks force your network team to perform a lot of repetitive, manual tasks — many of which are discouraged or require approvals given the implications of a mistake. If a line of business or a department requests a new application or service, you need to create VLANs, map VLANs across switches and uplinks, create port groups, update service profiles, and on and on.

Certain SDN models hope to help here by allowing programmatically controlled hardware, but this still leaves you with a lot of heavy lifting. For instance, you still need to build multiple identical physical network stacks to support your development, test, and production teams, and you still lack the ability to deploy your (hardware-based) network in lockstep with your virtualized compute and storage.

There's a high price tag associated with all of this. As Andrew Lerner, a Gartner research director, noted, "Configuration and change management of networking gear remains primarily a labor-intensive, manual process. These suboptimal network practices result in downtime, reduce security, degrade application performance, and waste human and capital resources."

Clearly, there's a better way forward: network automation. As *Network World* noted in a 2018 article, "Network automation is helping enterprises scale up and cut down on their costs exponentially, giving them the bandwidth needed to focus on strategy and innovation."

OpEx and CapEx are too high

The limitations of legacy network architectures are driving up data center costs — in terms of both operational expenditures (OpEx) and capital expenditures (CapEx).

OpEx

The heavy use of manual processes drives up the cost of network operations. Just consider all the labor-intensive manual tasks required to configure, provision, and manage a physical network. Now multiply the effort of these tasks across all the environments you need to support: development, testing, staging, and production; differing departmental networks; differing application environments; primary and recovery sites; and so on. Tasks that may be completed in minutes with automated processes — or even instantaneously with *automatic* deployment of networks — take hours, days, or weeks in a manual world.

And then there are the hidden costs that come with manually introduced configuration errors. One mistake can cause a critical connectivity issue or outage that impacts the business. Consider these findings:

- Studies by the Ponemon Institute consistently find that human error is one of the largest root causes for unplanned outages (Ponemon Institute Cost of Data Center Outages 2010, 2013, 2016).
- The financial effect of an unplanned data center outage can be huge. The Ponemon Institute found that the cost of an outage increased from $690,000 in 2013 to $740,000 in 2016, and has increased 38 percent since its 2010 study.

CapEx

On the capital side, legacy network architectures require your organization to invest in stand-alone solutions for many of the networking and security functions that are fundamental to data center operations. These include routing, firewalling, and load balancing. Providing these functions everywhere they're needed comes with a hefty price tag.

There is also the issue of the need to overprovision hardware to be sure you can meet peak demands, plus the need to deploy active–passive configurations. In effect, you need to buy twice the hardware for availability purposes, and sometimes much more.

And then there is the cost of forklift upgrades. To take advantage of the latest innovations in networking technology, network operators often have to rip and replace legacy gear, with most organizations on a three- to five-year refresh cycle. Legacy network architectures rooted in hardware also require overprovisioning to account for spikes in usage. The inability of hardware-based networks to scale automatically based on demands requires this inefficiency. And up goes the costs of networking.

Legacy network architectures can also result in other inefficiencies. Often, network designers must reserve parts of a network for a specific use to accommodate special security or compliance requirements. Coupled with the need for overprovisioning, the inefficiencies are magnified, leading to swaths of "dark servers" — and their associated networking resources — kept around "just in case" without serving any useful purpose. The result looks like a badly fragmented hard drive.

You can't leverage hybrid cloud resources

The public cloud model has proven that applications and services can be provisioned on demand. Enterprises everywhere would like to enjoy the same level of speed and agility. With that thought in mind, forward-looking executives envision using hybrid clouds for all kinds of use cases, from data storage and disaster recovery to software development and testing.

But, once again, there is a network-related catch: In their quest to move to the cloud, enterprises are hampered by vendor-specific network hardware and physical topology. These constraints that come with legacy data center architectures can make it difficult to implement hybrid clouds. Hybrid clouds depend on a seamless extension of the on-premises data center to a public cloud resource, and how do you achieve this when you can't control the public cloud network to mirror your hardware networking systems?

Networks have inadequate defenses

Many of the widely publicized cyberattacks of recent years share a common characteristic: Once inside the data center perimeter, malicious code moved from server to server, where sensitive data was collected and sent off to cybercriminals. These cases highlight a weakness of today's data centers: They have limited network security controls to stop attacks from spreading inside the data center.

Perimeter firewalls are pretty good at stopping many, but not all, attacks. As the recent attacks have shown, threats are still slipping into the data center through legitimate access points. Once inside, they spread like a deadly viral disease. This has been a tough problem to solve because of the realities of physical network architectures. Put simply, with legacy networking systems, it's too costly to provide firewalling for traffic between *all* workloads inside the data center. That makes it hard to stop an attack from laterally propagating from server to server using east–west traffic.

REMEMBER

To this point, we've noted that:

- To stay competitive, businesses need to move fast, yet their networks don't have the agility they need.
- Antiquated network architectures are blocking the road to the SDDC and virtual cloud network.
- Legacy network architectures limit business agility, leave security threats unchecked, and drive up costs.

These themes point to a single overarching need: It's time to move out of the hardwired past and into the era of the virtualized network.

IN THIS CHAPTER

- Explaining the basics of network virtualization
- Highlighting the benefits of this new approach
- Outlining key characteristics of a virtualized network

Chapter 2
It's Time to Virtualize the Network

In this chapter, we dive into the concept of network virtualization — what it is, how it differs from other approaches to the network, and why the time is right for this new approach.

To put things in perspective, let's begin with a little background on network virtualization, the state of today's networks, and how we got to this point.

How Network Virtualization Works

Network virtualization makes it possible to programmatically create, provision, and manage networks all in software, while continuing to leverage the underlying physical network as the packet-forwarding backplane. Network and security services in software are distributed to a virtual layer (hypervisors, in the data center) and "attached" to individual workloads, such as your virtual machines (VMs) or containers, in accordance with networking and security policies defined for each connected application. When a workload is moved to another host, its networking and security services move with it. And when new workloads are created to scale an application, the necessary policies are dynamically applied to those as well.

Similar to how a VM or a container is a software construct that presents logical services to an application, a *virtual network* is also a software construct that presents logical network services — switching, routing, firewalling, load balancing, virtual private networks (VPNs), and more — to connected workloads. These network and security services are delivered in software and require only Internet Protocol (IP) packet forwarding from the underlying physical network. The workloads themselves are connected via the logical network, implemented by overlay networking. This allows for the entire network to be created in software (see Figure 2-1).

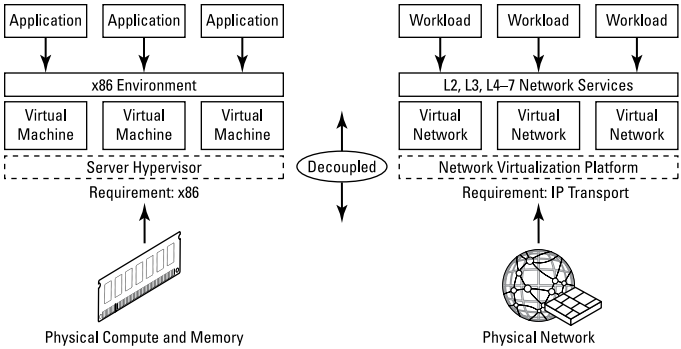


FIGURE 2-1: Compute and network virtualization.

Network virtualization coordinates the virtual switches across the various environments (for example, hypervisors, clouds) along with the network services (for example, firewalling, load balancing), to effectively deliver a networking platform and the creation of dynamic virtual networks (see Figure 2-2).

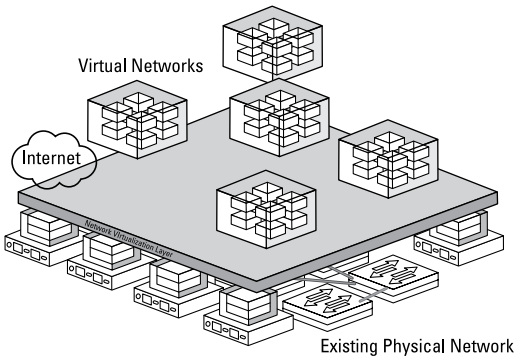


FIGURE 2-2: The network virtualization platform.

Another advantage of network virtualization is that network resources and services can be provisioned through a number of interfaces. One set of options makes use of the native user interfaces — the native graphical user interface (GUI) and command-line interface (CLI). Another approach leverages the application programming interface (API) to script or bake in homegrown tools. New application frameworks like Kubernetes integrate with network virtualization so networking services are created as new apps, pods, and containers that are spun up. Another way to provision virtual networks uses a cloud management platform (CMP) — such as OpenStack or VMware vRealize Automation — to request a virtual network and the appropriate security services for new workloads. In each case, the controller distributes the necessary network services to the corresponding virtual switches and logically attaches them to the corresponding workloads (see Figure 2-3).

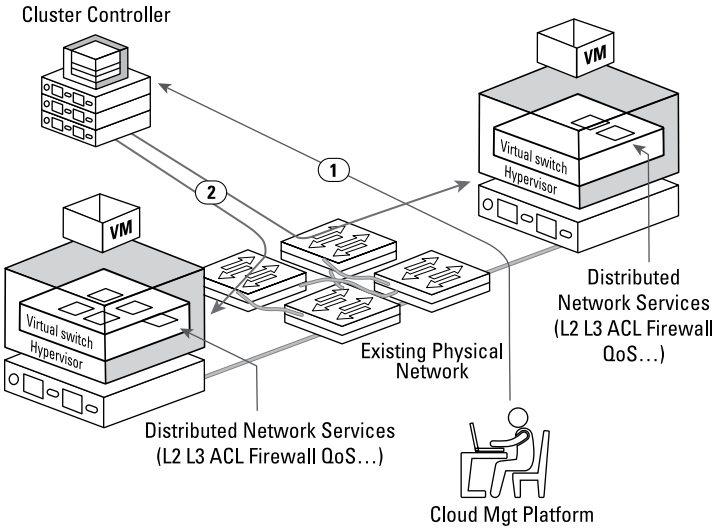


FIGURE 2-3: Virtual network provisioning.

This approach not only allows different virtual networks to be associated with different workloads in the same environment (for example, cluster, pod, hypervisor, application instance, virtual private cloud [VPC]), but it also enables the creation of everything

from basic virtual networks involving as few as two nodes to very advanced constructs that match the complex, multi-segment network topologies used to deliver multitier applications.

To connected workloads, a virtual network looks and operates like a traditional physical network (see Figure 2-4). Workloads "see" the same layer 2, layer 3, and layer 4 through layer 7 network services that they would in a traditional physical configuration. It's just that these network services are now logical instances of distributed software modules running in software on the local host and applied at the virtual interface of the virtual switch.

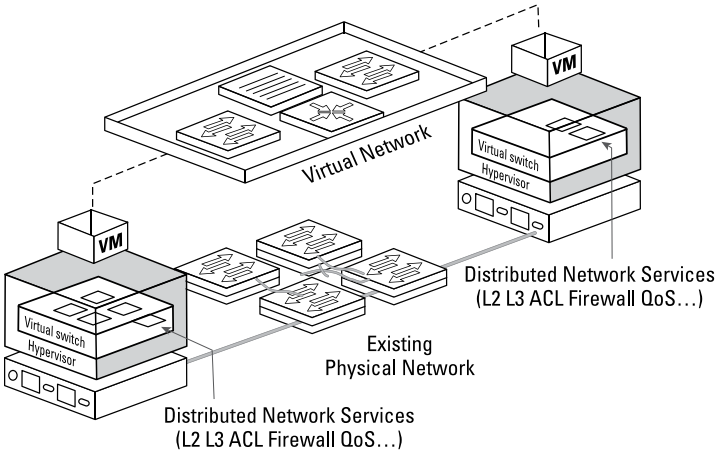


FIGURE 2-4: The virtual network, from the workload's perspective (logical).

To the physical network, a virtual network looks and operates like a traditional physical network (see Figure 2-5). The physical network "sees" the same layer 2 network frames that it would in a traditional physical network. The virtualized workload sends a standard layer 2 network frame that is encapsulated at the source hypervisor with additional IP, user datagram protocol (UDP), and logical network overlay headers (for example, virtual extensible local area network [VXLAN] or generic network virtualization encapsulation [GENEVE]). The physical network forwards the frame as a standard layer 2 network frame, and the destination

environment (for example, hypervisor, container platform, cloud) decapsulates the headers and delivers the original layer 2 frame to the destination workload (for example, VM or container).

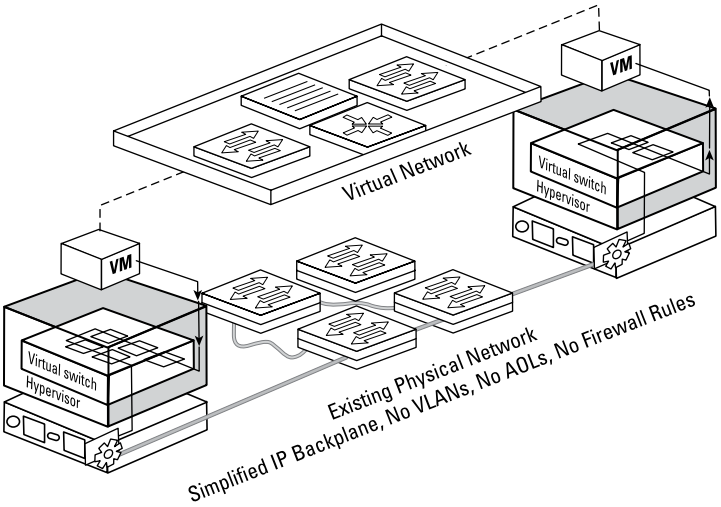


FIGURE 2-5: The virtual network, from the network's perspective (physical).

The ability to apply and enforce security services at the virtual interface of the virtual switch also eliminates "hairpinning" (see Chapter 3) in situations where east–west traffic between two endpoints on the same physical host, but in different subnets, is required to traverse the network to reach essential services, such as routing and firewalling.

WHAT'S THE DIFFERENCE BETWEEN A VIRTUAL NETWORK AND A VIRTUAL LOCAL AREA NETWORK?

If you work in networking, you know all about virtual local area networks (VLANs). They've been around for a long time. So, why aren't VLANs sufficient? Let's look at the differences between VLANs and virtual networks.

(continued)

(continued)

The VLAN approach breaks up a physical local area network (LAN) into multiple virtual networks. Groups of ports are isolated from each other as if they were on physically different networks. The VLAN approach is like slicing a big network pie into a lot of bite-size networks. Looking ahead, as your network grows, you could eventually run into a dead end: the limitation of 4,096 total VLANs in a single LAN.

The problems with VLANs don't stop there. Another big limitation is that VLANs don't allow you to save, snapshot, delete, clone, or move networks. And then there is the inherent security issue with VLANs — they don't allow you to control traffic between two systems on the same VLAN. This means that an attack that hits one system can jump to another system.

VLANs don't deliver a holistic approach to virtualizing the network. This means that

- Configuration is required at every physical and virtual hop to extend a VLAN.
- They tackle only segmentation of layer 2 networks, which has immense unnecessary complexity consequences for other networking services, such as routing, firewalling, and load balancing.

Network virtualization is far more than VLANs, making possible the creation of entire networks in software — including switching, routing, firewalling, and load balancing, doing so closer to the app, and orchestrating the process by default. This approach provides far greater flexibility than was possible in the past. With all networking and security services handled in software and attached to the application, labor-intensive management and configuration processes can be streamlined and automated, and networks can be created automatically to meet workload demands.

Network Virtualization and Software-Defined Networking

Network virtualization may sound a lot like software-defined networking (SDN), so what's the difference? Let's look at these two concepts.

The term *software-defined networking* means different things to different people, but it all started with the goal of making the network more agile by defining networking constructs in software. In this regard, network virtualization and SDN are similar. How SDN has manifested itself varies widely. In some instances, the goal is to manage the configuration of physical network devices. In others, it's about the broader orchestration of the network services by tying multiple systems together via APIs (some software, some hardware). In many cases, hardware remains the driving force for the network, which gets away from the original goal.

Network virtualization has a more specific definition, and completely decouples network resources from the underlying hardware. Networking components and functions are replicated in software. Virtualization principles are applied to physical network infrastructure to create a flexible pool of transport capacity that can be allocated, used, and repurposed on demand.

With your networking resources decoupled from the physical infrastructure, you basically don't have to touch the underlying hardware when adding or updating applications, regardless of the networking services they require. Endpoints can move from one logical domain to another without anyone having to reconfigure the network or wire up domain connections. You implement network virtualization in a virtual layer within the compute domain — close to the application — rather than on network switches. As noted earlier, the physical network, very critical still, serves as a packet-forwarding backplane, but is not required to change with each application change.

REMEMBER

SDN originally shared the same goal as network virtualization — making the network more agile — but SDN is a broader term that has taken on a number of various definitions, many of which are tied to hardware architectures, and many of which do not fully virtualize the network.

Virtual Appliances versus Integration in the Virtual Layer

Many providers of networking and security services have realized that what was traditionally offered with a physical appliance must come closer to the application to be more agile and more effective.

To that end, these providers are also offering virtualized options. These are referred to as *virtual appliances.* Virtual appliances are usually designed to deliver the functionality of a single network function, such as a router, a wide area network (WAN) accelerator, or a network firewall, but in the form factor of a dedicated VM.

Though they meet targeted needs, virtual appliances have some different characteristics from a broader network virtualization approach. For starters, virtual appliances run as guests on top of a hypervisor, which limits performance. They also introduce the challenge of virtual appliance sprawl. Because of the limited performance of the devices, you may end up having to deploy tens, hundreds, or even thousands of virtual appliances to reach the scale of the full data center. This presents capital expenditure (CapEx) barriers, as well as operational challenges.

The real value of network virtualization emerges in the integration of all networking functions into a comprehensive virtual network layer that includes an orchestration (or controller) mechanism and deep integration with the virtual compute layer (for example, hypervisor, container orchestration, or cloud). This more sophisticated approach allows the network and the full range of its functions to follow VMs as they move from one server to another. There's no need to reconfigure any network connections, because those are all in software. Basically, the network can go anywhere that is virtualized.

There are many other advantages to the intrinsically virtual approach to network virtualization. We cover these in Chapter 3. For now, let's just say that this new approach to the network makes your data center, and app management beyond the data center, a lot more agile. It's kind of like going from hardwired to wireless connections on your home network. You're set free of a traditional constraint.

Why the Time Is Right for Network Virtualization

People have been talking about network virtualization for years. It's now time to let the rubber meet the road — to meet pressing needs in today's applications.

Here are some of the reasons why the time is right for network virtualization.

Meeting the demands of a dynamic business

Simply put, software moves faster than hardware. It's far easier to deploy services, make changes, and roll back to previous versions when the network is all in software. Today's businesses have constantly changing requirements, which puts increasing demands on IT to be able to support these changes. When the network environment is run purely in software, it's much more flexible in adapting to changes, making it possible for IT organizations to meet business demands more effectively.

Increasing flexibility with hardware abstraction

Network virtualization moves intelligence from dedicated hardware to flexible software that increases IT and business agility. This concept is known as *abstraction.* To explain this concept, let's start in the well-established world of server virtualization.

With server virtualization, an abstraction layer, or hypervisor, reproduces the attributes of the physical server — central processing unit (CPU), random access memory (RAM), disk, and so on — in software. Abstraction allows these attributes to be assembled on the fly to produce a unique VM.

Network virtualization works the same way. With network virtualization, the functional equivalent of a "network hypervisor" reproduces networking services — such as switching, routing, access control, firewalling, quality of service (QoS), and load balancing — in software. With everything in software, virtualized services can be assembled in any combination to produce a unique virtual network in a matter of seconds.

This level of agility is one of the big benefits of the software-defined data center (SDDC), extending to the virtual cloud network, and one of the big arguments for network virtualization.

Increasing security with micro-segmentation

Another argument for network virtualization revolves around the need for stronger security. Network virtualization increases security by serving as the foundational building block for *micro-segmentation:* the use of fine-grained policies and network control to enable security *for each application*. Micro-segmentation allows you to shrink-wrap security around each workload, preventing the spread of lateral threats. We explain more on this concept in Chapter 4.

With network virtualization, networks are isolated by default, which means that workloads on two unrelated networks have no possibility of communicating with each other. Isolation is foundational to network security, whether for compliance, containment, or simply keeping development, test, and production environments from interacting. When virtual networks are created, they remain isolated from each other unless you decide to connect them. They require no physical subnets, no VLANs, no access control lists (ACLs), and no physical firewall configuration to enable this isolation.

Virtual networks are also isolated from the underlying physical network. This isolation not only decouples changes in one virtual network from affecting another, but also protects the underlying physical infrastructure from attacks launched from workloads in any of your virtual networks. Once again, you don't need any VLANs, ACLs, or firewall rules to create this isolation. That's just the way it is with network virtualization.

TAKING A CLOSER LOOK AT MICRO-SEGMENTATION

For a deep dive into the concept of micro-segmentation, download a copy of *Micro-segmentation For Dummies* (Wiley) at `www.vmware.com/go/MicrosegmentationForDummies.com`. This tightly written book, sponsored by VMware, provides a close-up look at the concepts, technologies, and benefits of micro-segmentation with the VMware NSX family.

Establishing a platform for the software-defined data center

As we note in Chapter 1, the SDDC is a much-needed framework for greater IT agility and more responsive IT service delivery, all at a lower cost within the data center, and the virtual cloud network extends these concepts to applications everywhere.

Network virtualization is a transformative architecture that makes it possible to create and run entire networks in parallel on top of existing network hardware. This results in faster deployment of workloads, as well as greater agility and security in the face of increasingly dynamic data centers, clouds, and edge nodes.

Rethinking the Network

Though it leverages your existing network hardware, network virtualization is a fundamentally new approach to the network. This means you need to think about your network in new ways. In the past, network functions revolved all around hardware. Now they have all the flexibility of software.

A virtualized network should allow you to take an entire network, complete with all its configurations and functions, and duplicate it in software.

TIP

You should be able to create and run your virtualized network in parallel on top of your existing network hardware. A virtual network can be created, saved, deleted, and restored, just as you would do with VMs, but in this case you're doing it with the entire network.

REMEMBER

In more specific terms, a virtualized network gives you the ability to

- Decouple the network from underlying hardware and apply virtualization principles to network infrastructure.
- Create a flexible pool of transport capacity that can be allocated, used, and repurposed on demand.
- Deploy networks in software that are fully isolated from each other, as well as from other changes in the data center.

- Transfer, move, and replicate the network, just as you can do with virtualized compute and storage resources.
- Make consistent network functionality available anywhere in your enterprise.

So, how do you get there? We cover that part of the story in Chapter 3, where we explore the technologies behind network transformation.

IN THIS CHAPTER

- Explaining the key functionality of a virtualized network
- Introducing the technologies for network virtualization
- Outlining key features of a virtualized network
- Exploring functional and economic benefits

Chapter 3
Transforming the Network

In the previous chapters, we introduce network virtualization and provide a quick overview. In this chapter, we dig deeper into the technologies you need in order to bring the benefits of virtualization to your network environment. We begin by introducing the concepts behind network virtualization and conclude with details of VMware NSX Data Center, a multi-hypervisor, multi-cloud network virtualization and security platform.

The Key Functionalities of a Virtualized Network

Some of the key functionalities of a virtualized network include overlay networking, as well as the traditional functions you're probably more familiar with, like routing and load balancing, which are now done in software, closer to the application.

Overlay networks

Network virtualization makes use of overlay technologies, which sit above the physical network hardware, enabling a logical network, as shown in Figure 3-1.

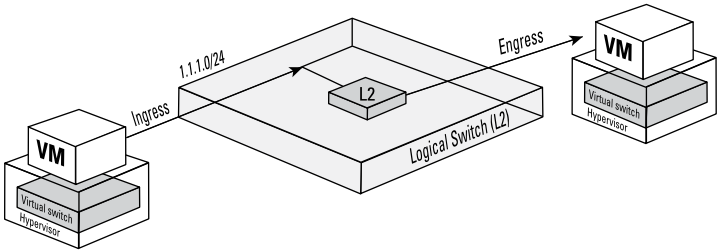


FIGURE 3-1: Logical networking via the use of overlays.

Network overlays make it possible to run networks entirely in software, abstracted from the supporting physical network infrastructure. In the case of the data center network, they create tunnels between endpoints within the virtual layer.

Packet flow from sender to receiver

As we note elsewhere, virtual networks use the underlying physical network as the packet-forwarding backplane, and bring more nuanced networking decisions closer to the application. When application endpoints (for example, two virtual machines [VMs]) communicate with each other, the packet is encapsulated with the Internet Protocol (IP) address of the destination virtual endpoint. The physical network delivers the frame to the destination host or hypervisor, which can remove the outer header, and then the local virtual switch instance delivers the frame to the destination application endpoint.

In this way, the communication uses the underlying physical network as a simple IP backplane — one that doesn't require much complexity like Spanning Tree Protocol (STP) or access control lists (ACLs), as these things can now be done closer to the application by the network virtualization platform. This approach dramatically simplifies configuration management and eliminates physical network changes from the network provisioning process, which is a pretty big deal.

Overlay technologies

There are various overlay technologies. One industry-standard technology is called virtual extensible local area network (VXLAN). VXLAN provides a framework for overlaying virtualized layer 2 networks over layer 3 networks, defining both an encapsulation mechanism and a control plane. Another is generic network virtualization encapsulation (GENEVE), which takes the same concepts but makes them more extensible by being flexible to multiple control plane mechanisms.

There are also others, including network virtualization using generic routing encapsulation (NVGRE). NVGRE is similar to VXLAN in its goals, but it uses different approaches to create the overlay. NVGRE has had limited adoption in comparison to the momentum of VXLAN and GENEVE.

A primer on VXLAN and GENEVE

This section fills you in on VXLAN and GENEVE — how they're similar and how they're different.

Encapsulation

VXLAN and GENEVE are both overlay technologies encapsulating the original Ethernet frames generated by workloads (virtual or physical) connected to the same logical layer 2 segment, usually named a logical switch. They are also both layer 2 over layer 3 (L2oL3) encapsulation technologies. The original Ethernet frame generated by a workload is encapsulated with an external header, followed by the User Datagram Protocol (UDP), IP, and Ethernet headers to ensure that it can be transported across the network infrastructure interconnecting the VXLAN or GENEVE endpoints (typically the application endpoint, such as a VM or container pod).

Scaling

Extending beyond the 4,096 virtual local area network (VLAN) limitation on traditional switches is achieved by leveraging a 24-bit identifier, named a VNI (VXLAN network identifier in VXLAN, or virtual network identifier in GENEVE), which is associated with each layer 2 segment created in the logical space. This value is carried inside the overlay header and is normally associated with an IP subnet, similar to what traditionally happens with VLANs. Intra-IP subnet communication happens between devices connected to the same virtual network (logical switch).

Traversing the network

Hashing of the layer 2, layer 3, and layer 4 headers present in the original Ethernet frame is performed to derive the source port value for the external UDP header. This is important to ensure load balancing of overlay traffic across equal-cost paths potentially available inside the transport network infrastructure.

Terminating the tunnels

The source and destination IP addresses used in the external IP header uniquely identify the hosts originating and terminating the overlay encapsulation of frames. This functionality lies within the tunnel endpoint (in GENEVE) or VXLAN Tunnel EndPoint (VTEP, in VXLAN).

Frame size

Encapsulating the original Ethernet frame into a UDP packet increases the size of the IP packet. This results in one of very few requirements for the physical network infrastructure: It's recommended to increase the maximum transmission unit (MTU) size to a minimum of 1,700 bytes on all interfaces that will carry overlay network traffic. The MTU for the virtual switch uplinks of the tunnel endpoints performing the VXLAN or GENEVE encapsulation is automatically increased when preparing the tunnel endpoint for VXLAN or GENEVE.

Figure 3-2 describes (at a high level) the steps required to establish layer 2 communications between application endpoints leveraging overlay functionality — in this case, let's say two VMs communicating over VXLAN:

- VM1 originates a frame destined to the VM2 part of the same layer 2 logical segment (IP subnet).
- The source VTEP identifies the destination VTEP where VM2 is connected and encapsulates the frame before sending it to the transport network.
- The transport network is required only to enable IP communication between the source and destination VTEPs.
- The destination VTEP receives the VLXLAN frame, de-encapsulates it, and identifies the layer 2 segment to which it belongs.
- The frame is delivered to VM2.

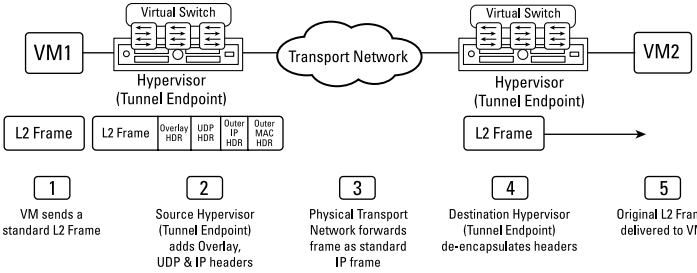


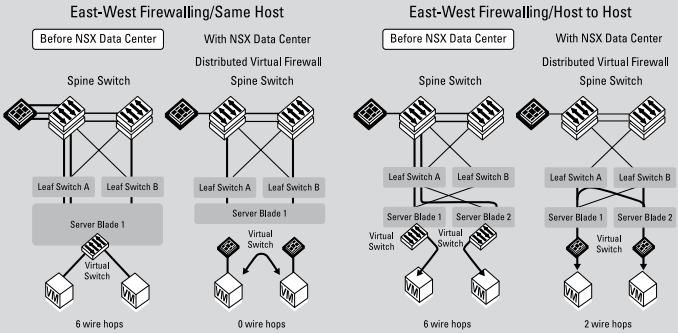
FIGURE 3-2: Establishing layer 2 communication between VMs with VXLAN.

NETWORK VIRTUALIZATION IN ACTION: AN EXAMPLE

Here's one of many potential examples of how network virtualization makes life better for your security and network administrators.

Communication on a conventional network can be inefficient when services, such as firewalling, are applied. Traffic must be routed out of the virtual environment, passed through the physical firewall, and then redirected back to the virtual environment. This process is often referred to as *hairpinning* or *tromboning* — basically, it goes out just to come back, before even reaching its destination. It adds complexity and latency, lowering performance and increasing instability, and making it harder for application endpoints to move.

By contrast, when network services are integrated into a network virtualization layer, there's no need for this hairpinning process. These concepts are illustrated in the following figure.



Virtual Network Functions

Overlay networking is pretty powerful, but it's only a piece of the network virtualization story. Overlays basically enable you to now make networking decisions in software, in a virtual layer, abstracted from the physical hardware with all the benefits that come with. But then what? What do those decisions look like? That's where virtual network functions come in. In fact, many of them can realize benefits without deploying overlay networking.

What functions? Well, how IP networking works isn't necessarily changing, so you still need a router in the virtual space. Because you're bringing networking closer to the application, it might benefit from a new model for load balancing, too. These can be centralized functions (think a single router) or distributed functions (as has been done for years with virtual distributed switching). Finally, something that has really revolutionized security is the virtual distributed firewall. We get into each of these functions more as we go through architectures and use cases.


TECHNICAL STUFF

Virtual Network Functions, with a capital *V*, capital *N*, and capital *F*, is a key term in the realm of Network Function Virtualization (NFV). This realm is one focused on virtualizing the physical network functions required by service provider networks and mobile carrier networks. In fact, it's very similar to how functions are moving into software in the data center space and elsewhere, but it's also still distinct in many ways, so it's worth clarifying that we're not necessarily talking about NFV here, even though we're discussing bringing network functions into software.

The Big Payoff

Network virtualization helps organizations achieve major advances in speed, agility, and security by automating and simplifying many of the processes that go into running a data center network and managing networking and security in the cloud.

Here's a quick checklist of some of the key benefits that come with this new approach to the network. Network virtualization helps you

- Reduce network provisioning time from weeks to minutes.
- Achieve greater operational efficiency by automating manual processes.
- Place and move workloads independently of physical topology.
- Improve network security within the data center.

Meet VMware NSX Data Center: Bringing Network Virtualization to the SDDC

First, a simple definition: VMware NSX is a family of networking products from VMware that realize network virtualization from the data center to the cloud to the edge. NSX Data Center is the network virtualization and security platform for the software-defined data center (SDDC). NSX Data Center reproduces the entire network model in software. This end-to-end model enables any network topology — from simple to complex multitier networks — to be created and provisioned in seconds. It delivers all the goodness of network virtualization that we've covered so far, and more, which we get to later.

While increasing agility and streamlining your approach to the network, NSX Data Center enhances security inside the data center. These security gains are delivered via automated fine-grained policies that wrap security controls around each application endpoint. This is a completely new approach. It enables an intrinsically secure network, preventing attacks that move laterally within the data center, jumping from workload to workload with little or no controls to block their propagation. With NSX Data Center, workloads can be isolated from each other, as though each were on its own network.

How It Works

In this section, we pop the latch and give you a look under the hood of VMware NSX Data Center.

NSX Data Center architecture

The NSX approach to network virtualization in the data center allows you to treat your physical network as a pool of transport capacity that can be consumed and repurposed on demand. Virtual networks are created, provisioned, and managed in software, using your physical network as a simple packet-forwarding backplane.

Virtualized network services are distributed to each application endpoint independently of the underlying network hardware or topology. This means workloads can be added or moved on the fly and all the network and security services attached to the app move with it, anywhere in the data center. Your existing applications operate unmodified. They see no difference between a virtual network and a physical network connection.

Integration with existing network infrastructure

NSX Data Center works with your existing compute and networking infrastructure, applications, and security products. You can deploy NSX Data Center nondisruptively on top of your current infrastructure.

Better still, NSX Data Center is not an all-or-nothing approach. You don't have to virtualize your entire network. You have the flexibility to virtualize portions of your network by simply adding hypervisors, bare-metal hosts, even clouds, to the NSX platform.

Simplified networking

After NSX Data Center is deployed, little interaction with the physical network is required. You no longer need to deal with the physical network configuration of VLANs, ACLs, spanning trees, complex sets of firewall rules, and convoluted hairpinning traffic patterns — because these are no longer necessary when the network is virtualized.

REMEMBER

As you deploy NSX virtual networks, you can increasingly streamline your physical network configuration and design. Vendor lock-in becomes a thing of the past because the physical network only needs to deliver reliable high-speed packet forwarding. This means you can mix and match hardware from different product lines and vendors.

Unlocking a broader ecosystem of networking and security capabilities

NSX Data Center is extremely flexible, highly extensible, and widely supported. A powerful traffic-steering capability, referred to as *service insertion*, allows any combination of network and security services to be chained together in any order. It's all defined by the application policies you set for each workload.

This high degree of flexibility applies not only to native NSX Data Center services but also to a wide variety of compatible third-party solutions — including virtual and physical instances of next-generation firewalls, application delivery controllers, and intrusion prevention systems.

Let's take a step back and consider the bigger picture here. The availability of many NSX-compatible products from VMware partners is a sign of industry support for the new operational model delivered by the NSX Data Center platform. This gives you greater confidence as you move into the realm of the virtualized network. You have a broad ecosystem on your side. For more details, check out Chapter 6 and the "Integrating with Your Networking Services Ecosystem Partners" section.

What It Does: The Key Capabilities of NSX Data Center

Let's look at some of the key technical capabilities of VMware NSX Data Center. At the outset, keep this point in mind: NSX Data Center virtualizes all network functions. In addition, many that are covered, and many that are not, are also available from the ecosystem of partners. In this sense, NSX is like a magic layer that enables a spectrum of capabilities across your environment.

Everything in software

REMEMBER

Here are some of the key features of VMware NSX Data Center:

- **Logical distributed switching:** NSX Data Center allows you to reproduce the complete layer 2 and layer 3 switching functionality in a virtual environment, decoupled from the underlying hardware.

- **NSX gateway:** This layer 2 gateway enables seamless connection to physical workloads and legacy VLANs.
- **Logical routing:** Routing between logical switches provides dynamic routing within different virtual networks.
- **Logical distributed firewalling:** NSX Data Center allows you to create a distributed firewall, integrated into the virtual networking layer and wrapping security around each workload. This comes full with layer 7 application identification, as well as user-based firewalling.
- **Logical load balancer:** NSX Data Center provides a full-featured load balancer with SSL termination.
- **Logical VPN:** NSX Data Center supports site-to-site and remote access virtual private networks (VPNs) in software.
- **NSX API:** This RESTful API enables integration into any cloud management platform.
- **Integration with cloud management platforms:** Integration is enabled with fully baked automation through platforms like OpenStack or VMware vRealize Automation.
- **Service insertion:** NSX Data Center enables you to plug in functions from third-party services, not only as a northbound API call, but as a chained service for each packet flow.
- **Multi-site, multi-cloud networking and security:** You can extend these concepts outside a single data center domain to multiple sites and clouds.
- **Planning, visibility, and operations tools:** Tools like Application Rule Manager allow you to capture traffic and use this visibility to create network policies, while Traceflow allows you to do a packet walk for debugging, for example.

Essential isolation, segmentation, and advanced security services

Every year, businesses spend billions of dollars to secure the perimeters of their data centers. And guess what? Breaches continue to mount. Though it is an essential part of a security strategy, perimeter protection doesn't do everything you need. We need a new model for data center security. Micro-segmentation, a concept introduced in Chapter 2, provides this model.

NSX Data Center brings security inside the data center with automated fine-grained policies tied to application endpoints, such as VMs. Network security policies are enforced by firewalling controls integrated into the virtual layer, such as the hypervisor, that is already distributed throughout the data center. The hypervisor, for example, serves as an ideal place to enforce such policies — it's close to, yet isolated from, the application. These security policies move when VMs move and adapt dynamically to changes in your data center.

Virtual networks can operate in their own address spaces or have overlapping or duplicate address spaces — all without interfering with each other. Virtual networks are inherently isolated from all other virtual networks, and the underlying physical network, by default. Each virtual network is like an island in a data center sea. This approach allows you to securely isolate networks from each other. You end up with an inherently better security model for the data center. Malicious software that slips through your firewall is no longer free to jump from server to server.

Of course, none of this means you have to give up your favorite network security solutions. NSX Data Center is a platform for bringing the industry's leading networking and security solutions into the SDDC. Thanks to tight integration with the NSX Data Center platform, third-party products and solutions can be deployed as needed and can adapt dynamically to changing conditions in your data center.

REMEMBER

These network virtualization capabilities enable the three key functions of micro-segmentation:

- **Isolation:** No communication across unrelated networks
- **Segmentation:** Controlled communication within a network
- **Security with advanced services:** Made possible by tight integration with third-party security solutions

Performance and scale

NSX Data Center delivers proven performance and scale. Because networking functions are embedded in the virtual layer, NSX Data Center features a scale-out architecture that enables seamless scaling of additional capacity while also delivering solid availability and reliability.

Here's an example of the extreme scalability of NSX Data Center: In a real-world NSX Data Center deployment, a single cluster of controllers is being used to deliver more than 10,000 virtual networks, which in turn support more than 100,000 virtual machines. This isn't required by, nor does it make sense for, most networks, but many do have scalability limitations that are now addressed.

TECHNICAL STUFF

In the NSX Data Center environment:

- The processing required for the execution of distributed network services is incremental to what the vSwitch is already doing for connected workloads.
- The vSwitch is a module that is integrated with the hypervisor kernel, along with all the NSX Data Center network and security services.
- Virtual network transport capacity scales linearly (alongside app endpoint, or VM capacity) with the introduction of each new hypervisor/host, adding 20 Gbps of switching and routing capacity and 19.6 Gbps of firewalling capacity.

Unparalleled network visibility

NSX Data Center takes visibility into the network to an all-new level. With conventional approaches to networking, configuration and forwarding state are spread across lots of disparate network devices. This fragmentation can cloud your view and complicate troubleshooting.

By contrast, NSX Data Center provides all configuration and state information for all network connections and services in one place. Connectivity status and logs for all NSX Data Center components and virtual network elements (logical switches, routers, and the like) are readily accessible, as is the mapping between virtual network topologies and the underlying physical network. This enables full visibility of traffic between app endpoints — even when the communicating VMs or containers are on the same host and network traffic never reaches the physical network.

REMEMBER

Better yet, with NSX Data Center, you have access to advanced troubleshooting tools like Traceflow. This function injects a synthetic packet into a virtual switch port, providing the opportunity to observe the network path as it traverses physical and logical network systems. This allows your administrators to identify the

full path a packet takes and troubleshoot any points along the way where the packet is dropped (for instance, because of firewall policies).

This level of visibility isn't possible if you're running traditional physical networking hardware, and it definitely wouldn't be possible with physical networking in situations where two VMs are communicating on the same host.

The Key Benefits of VMware NSX Data Center

Now we're getting to the really good stuff. This section looks at some of the ways your organization can cash in on the capabilities of network virtualization with VMware NSX Data Center. You can break the story into two camps: functional benefits and economic benefits.

Functional benefits

The functional benefits of NSX Data Center revolve around four pillars of the SDDC: speed, agility, security, and reliability. Here's how these benefits are delivered:

- **Creating entire networks in software in seconds:** NSX Data Center arms you with a library of logical networking elements and services, such as logical switches, routers, firewalls, load balancers, VPN, and workload security. You can mix and match these components to create isolated virtual network topologies in seconds.
- **Minimizing the risk and impact of data breaches:** You can use NSX Data Center to isolate workloads, each with its own security policies. This capability helps you contain threats and block the movement of malicious software within your data center. Better internal security can help you avoid or reduce the costs of data breaches.
- **Speeding IT service delivery and time to market:** With network virtualization, you can reduce the time required to provision multitier networking and security services from weeks to minutes. Some enterprises use NSX Data Center to give application teams full self-service provisioning

capabilities. Even better, the automation and orchestration capabilities in NSX Data Center help you avoid the risk of manual configuration errors.

- **Simplifying network traffic flows:** You can use NSX Data Center to lessen the load of server-to-server traffic (east–west traffic) on the oversubscribed core. With a virtual network, VMs communicate with one another through the vSwitch or aggregation fabric. This cuts down on east–west traffic hops and helps you avoid the pitfalls of convoluted traffic patterns. The idea is to make better use of your current assets and avoid the costs of building up core capacity with more hardware.
- **Increasing service availability:** Cloud-scale data centers have few outages because they have flatter fabrics with equal-cost multipath routing between any points on the network. Simplified leaf-spine fabrics make individual links or devices inconsequential. The network can withstand multiple simultaneous device failures with no outage. With the network virtualization capabilities of NSX Data Center, you can achieve the same high availability in your data center.

Economic benefits

The economic benefits of network virtualization with NSX Data Center emerge in the form of savings on both capital and operational expenditures:

- **Reducing the risk of costly breaches:** Historically, deploying firewalls to control an increasing volume of east–west traffic inside the data center has been cost-prohibitive for many enterprises. What's more, the sheer number of devices needed and the effort required to set up and manage a complex matrix of firewall rules have made this approach operationally not feasible. The micro-segmentation capabilities that come with network virtualization make this all not just doable but affordable. You can now reduce the risk of cross–data center security breaches while avoiding high-dollar capital expenditures for additional hardware and software.

- **Reducing time and effort:** Network virtualization can greatly reduce the effort and time it takes to complete network tasks. Generally, NSX Data Center reduces the effort from hours to minutes, and the cycle times from days to minutes. If you consider all the manual tasks required to provision and manage a physical network — across development, testing, staging, and production environments — and the fact that NSX Data Center automates these, you begin to see lots of opportunities to reduce operational costs.
- **Improving server asset utilization:** In traditional topologies, each network cluster has its own compute capacity. IT admins often overprovision compute to avoid the lengthy, error-prone network reconfiguration required to reach available capacity in another cluster. NSX Data Center gives you a better way to get things done. You can use NSX Data Center to bridge two or more network clusters and deploy workloads to the unused capacity. By making better use of existing server capacity, you can avoid the need to buy new physical servers.
- **Improving price/performance savings:** Many enterprises are using the capabilities of NSX Data Center and network virtualization to replace expensive proprietary hardware with lower-cost infrastructure that can be bought from various vendors — whoever has the best price/performance.
- **Extending the hardware life cycle:** You can use NSX Data Center to pull more value from your existing network infrastructure. Here's how: NSX Data Center offloads an increasing volume of east–west traffic from the network core. This allows you to extend the hardware lifespan without having to add expensive capacity. With NSX Data Center, the underlying network hardware becomes a simple IP-forwarding backplane. Rather than refresh your networking gear at the end of the accounting depreciation cycle, you can use it for longer periods. With this approach, you touch the hardware only to add more capacity or to replace individual devices when they fail.

IN THIS CHAPTER

- Reevaluating security
- Driving automation
- Understanding multi-cloud networking

Chapter 4
Network Virtualization Use Cases

Network virtualization improves on the status quo both deeply, creating a big impact, as well as broadly, across a number of categories. In this chapter, we walk through those categories, giving a series of examples of how people are putting network virtualization into action.

REMEMBER

As you explore these use cases, keep this point in mind: As we note in Chapter 3, virtualization with NSX Data Center is not an all-or-nothing approach. You don't have to virtualize your entire network. You can virtualize portions of your network for targeted use cases and then expand your use of virtualization over time.

And here's a cool fact: Enterprises can often justify the cost of NSX Data Center through a single use case — while they establish a strategic platform that automates IT and drives additional use cases and projects over time.

In the following sections, we drill down into some of the more common use cases, to show how you can use network virtualization to speed up processes, strengthen security, and keep your applications up and running.

Securing the Data Center

As we note elsewhere, security is a huge and ever-growing concern for enterprises. Network virtualization provides an ideal layer for security — close to yet isolated from applications — that allows for a new infrastructure architecture with intrinsic security, drastically mitigating the risks of data breaches.

Micro-segmentation: Limiting lateral movement within the data center

Modern attacks exploit inherent weaknesses in traditional perimeter-centric network security strategies to infiltrate enterprise data centers. After successfully evading the data center's perimeter defenses, an attack can move laterally within the data center from workload to workload with little or no controls to block its propagation.

Micro-segmentation of the data center network restricts unauthorized lateral movement but, until now, hasn't been operationally feasible in data center networks because of the characteristics of traditional firewalls.

Traditional packet-filtering and advanced next-generation firewalls implement controls as physical or virtual choke points on the network. As application workload traffic passes through these control points, network packets are either blocked or allowed to traverse the firewall based on the firewall rules that are configured at that control point.

There are two key operational barriers to micro-segmentation using traditional firewalls: throughput capacity and security management. More important, they usually don't leverage network virtualization as a new ideal layer to implement and enforce security.

Limitations on transport capacity can be overcome, but at a significant cost. It's possible to buy enough physical or virtual firewalls to deliver the capacity required to achieve micro-segmentation, but in most (if not all) organizations, purchasing the number of firewalls necessary for effective micro-segmentation isn't financially feasible. We're effectively talking about a separate firewall per virtual machine (VM). How many VMs does your data center

have? Hundreds? Thousands? This would mean potentially thousands of firewalls for a typical data center.

The burden of security management also increases exponentially with the number of workloads and the increasingly dynamic nature of today's data centers. If firewall rules need to be manually added, deleted, and/or modified every time a new VM is added, moved, or decommissioned, the rate of change quickly overwhelms IT operations. It's this barrier that has been the demise of most security teams' best-laid plans to realize a comprehensive micro-segmentation or least-privilege unit-level trust strategy in the data center. (We discuss the concept of least privilege later in this chapter.)

The software-defined data center (SDDC) leverages a network virtualization platform to offer several significant advantages over traditional network security approaches. These include automated provisioning, automated move/add/change for workloads, distributed enforcement at every virtual interface, and in-kernel, scale-out firewalling performance, distributed to every hypervisor and baked into the platform.

The growth of east–west traffic within the data center

Over the past decade, applications have increasingly been deployed on multitier server infrastructures, and east–west server-to-server communications now account for significantly more data center traffic than north–south client-to-server and Internet communications. In fact, traffic inside the data center now accounts for as much as 80 percent of all network traffic. These multitier application infrastructures are typically designed with little or no security controls to restrict communications between systems.

Attackers have modified their attack strategies to take advantage of this paradigm shift in data center traffic, as well as the fact that prevailing perimeter-centric defense strategies offer little or no controls for network communications within the data center. Security teams must likewise extend their defense strategies inside the data center — where the vast majority of network traffic actually exists and is unprotected — instead of focusing almost exclusively on perimeter defenses.

Visibility

The growth of east–west traffic within the data center and the rise of server virtualization are two trends that have contributed to an alarming lack of visibility and context in the data center.

For the most part, east–west server communications in the data center do not pass through a firewall and are, therefore, not inspected. For all intents and purposes, this traffic is invisible to network security teams. When east–west traffic *is* forced through a firewall — using techniques such as hairpinning to backhaul the traffic through a firewall choke point — the result is a complex and inefficient communication path that hurts network performance throughout the data center.

Innovation in server virtualization has far outpaced the underlying network and security constructs in traditional data centers. Deploying multiple virtual workloads on a single physical host configured with multiple network interface cards (NICs) is common in virtual server environments. Without virtual switches, the traffic going to and from individual VMs cannot be easily identified. This can cause significant issues for network teams attempting to identify and troubleshoot problems and is fertile ground for an attacker.

The virtual network layer is uniquely positioned to see all traffic in the data center, down to the level of individual virtualized workloads (for example, VMs and containers). This level of visibility and context enables micro-segmentation based on attributes that are unique to each workload, such as the operating system, patch level, running services, and many other properties. This capability, in turn, enables more intelligent network and security policy decisions that can be defined with an understanding of the specific purpose of each individual workload in the data center.

For example, unique policies can be specifically defined for the web tier of an order-taking application, or for an enterprise human resources management system, based on the needs of the individual workload rather than the constraints of the underlying network topology.

Taking things a step further, not only does NSX Data Center provide visibility into network traffic by default, but it also offers tools to debug (for example, Traceflow) and build micro-segmentation

strategies based on that visibility (for example, Application Rule Manager), allowing you to implement policies in just a few clicks.

Context-aware

Traditional network security policies have necessarily been based on infrastructure constructs like Internet Protocol (IP) addresses and Transmission Control Protocol (TCP) ports that are more a result of static infrastructure than the context of the application. By bringing security close to the application, integrating with virtualization hypervisors and cloud platforms, network virtualization enables security policies that are, indeed, based on the context of the application. This is not only inherently more secure (because it gets to the point of the policy rather than an infrastructure artifact) but also easier to manage (because you no longer have to manage a number of layers of abstractions in order to write or understand a policy).

Here are some examples of application context that you might actually like to base a security policy on:

- **Workload context:** What operating system (OS) is the application running on? How have you labeled this workload using your internal tags?
- **User contexts:** Who is accessing this server? Should they be? What role do they have according to your Active Directory schema?
- **Application behavior:** What is the application doing? Is this a SQL query or an authentication or web traffic? This is best identified at layer 7, past the layer 4 port, which can only take a best guess, but of course it will be used to throw you off in the case of a malicious attack.
- **Third parties:** What do third-party systems have to say about this application, beyond the rich context that the network virtualization platform, cloud platform, or hypervisor already knows?

Isolation

Isolation is an important principle in network security, whether for compliance, containment, or simply keeping development, test, and production environments separated. Manually configured and maintained routing, access control lists (ACLs), and/or

firewall rules on physical devices have traditionally been used to establish and enforce isolation in data center networks.

Forrester Research outlines its Zero Trust model of information security and isolation, in which perimeter security controls are extended throughout the entire data center. This model requires organizations to protect external and internal data resources and enforce strict access controls. Zero Trust incorporates the principle of *least privilege*, a cornerstone of information security that limits access and permissions to the minimum required to perform an authorized function. Finally, the "trust, but verify" concept is so 1980s (with respect to, and apologies to, President Ronald Reagan). "Never trust, always verify" is the new paradigm for a safe and secure world.

Virtual networks are inherently isolated from other virtual networks and from the underlying physical network by design. This concept is distinctly different from the legacy approach of assuming some default level of trust within the data center. Isolation is inherent to network virtualization — no physical subnets, virtual local area networks (VLANs), ACLs, or firewall rules are required in order to enable this isolation. Virtual networks are created in isolation and remain isolated unless deliberately and explicitly connected.

Here is something else that is critical with this approach: Firewall policies in the distributed firewall, although closer to the application and leveraging application context, are also isolated from attacks because they don't sit in the guest. They run in the kernel, in the hypervisor.

Any isolated virtual network can be made up of workloads distributed anywhere in the data center, and workloads in the same virtual network can reside on the same or separate hypervisors. Additionally, workloads in several isolated virtual networks can reside on the same hypervisor. Isolation between virtual networks also allows for overlapping IP addresses. So, it's possible, for example, to have isolated development, test, and production virtual networks, each with a different application version, but with the same IP addresses, all operating at the same time on the same underlying physical infrastructure.

Finally, virtual networks are also isolated from the underlying physical infrastructure. Because traffic between hypervisors is

encapsulated, physical network devices operate in a completely different address space than the workloads connected to the virtual networks.

For example, a virtual network could support IPv6 application workloads on top of an IPv4 physical network. This isolation protects the underlying physical infrastructure from any possible attack initiated by workloads in any virtual network. Again, all this is independent from any VLANs, ACLs, or firewall rules that would traditionally be required in order to create this isolation.

Segmentation

Segmentation is related to isolation but applied within a multitier virtual network. Traditionally, network segmentation is achieved with a physical firewall or router that allows or denies traffic between network segments or tiers — for example, segmenting traffic between a web tier, application tier, and database tier. Segmentation is an important principle in security design because it allows organizations to define different trust levels for different network segments and reduces the attack surface should an attacker breach the perimeter defenses. Unfortunately, data center network segments are often far too large to be effective, and traditional processes for defining and configuring segmentation are time-consuming and prone to human error, often resulting in security breaches.

Network segmentation, like isolation, is a core capability of a network virtualization platform. A virtual network can support a multitier network environment — multiple layer 2 segments with layer 3 segmentation (or micro-segmentation) on a single layer 2 segment, using distributed firewalling defined by workload security policies. These could represent a web tier, an application tier, and a database tier, for example.

In a virtual network, network and security services — such as layer 2, layer 3, ACLs, firewall, and quality of service (QoS) — that are provisioned with a workload are programmatically created and distributed to the hypervisor virtual switch and enforced at the virtual interface. Communication within a virtual network never leaves the virtual environment, removing the requirement for network segmentation to be configured and maintained in the physical network or firewall.

Automation

Automated provisioning enables the correct firewalling policies to be provisioned when a workload is programmatically created, and those policies follow the workload as it moves anywhere in the data center or between data centers.

Equally important, if the application is deleted, its security policies are automatically removed from the system. This capability eliminates another significant pain point — firewall rule sprawl — which potentially leaves thousands of stale and outdated firewall rules in place, often resulting in performance degradation and security issues.

You can also apply a combination of different partner capabilities by chaining advanced security services together and enforcing different services based on different security situations. This enables your organization to integrate your existing security technologies to build a more comprehensive and correlated security capability inside the data center. Existing security technologies actually function better with micro-segmentation than otherwise possible, because they have greater visibility and context of individual workload VM traffic inside the data center, and security actions can be customized for individual VM workloads as part of a complete security solution.

For example, a workload may be provisioned with standard firewalling policies, which allow or restrict its access to other types of workloads. The same policy may also dictate that if a vulnerability is detected on the workload during the course of normal vulnerability scanning, a more restrictive firewalling policy would apply, restricting the workload to be accessed by only those tools used to remediate the vulnerabilities.

TIP

Security vendors can take advantage of the network virtualization platform to trigger advanced security service responses from a completely different security vendor's technology solution — an innovation that's accelerated with network virtualization.

Service insertion and guest introspection

As a foundational component of the infrastructure, NSX Data Center is uniquely positioned to empower other security solutions to better protect the environment. Next-generation firewalls

or intrusion prevention systems (IPSs) can be inserted inline and traffic can be dynamically steered by NSX Data Center to these systems, increasing traffic flow efficiency while maintaining security. For more details on integrating with your networking services ecosystem partners, see Chapter 6.

Secure user environments: Micro-segmentation for VDI

Many enterprises have deployed virtual desktop infrastructure (VDI) to leverage virtualization technologies beyond the data center. Micro-segmentation enables these organizations to extend many of the security advantages of the SDDC to the desktop — and even to mobile environments — including the following:

- Integrating key network and security capabilities into VDI management
- Eliminating complex policy sets and topologies for different VDI users
- Setting firewall and traffic filtering and assigning policies for logical groupings
- Decoupling security policies from the network topology to simplify administration

Through its capability to implement micro-segmentation, NSX Data Center effectively enables each virtual desktop to have its own firewall. This allows a much more granular level of security — that extends all the way down to the virtual network interface. Based on policies, all traffic to and from that VM can be secured, preventing unauthorized communication between VMs or other workloads. If an end-user's virtual desktop becomes compromised, the exposure can easily be contained to only that user.

Automating IT Processes

In large data centers, manual processes are the bane of the IT admin's existence and a drain on the manager's budget. Network virtualization helps you address these challenges by automating labor-intensive, error-prone tasks associated with network configuration, provisioning, management, and more.

IT automation

With NSX Data Center, powerful orchestration capabilities distribute network services in parallel with VMs. You can use NSX Data Center to standardize and maintain predefined templates that consist of network topologies and services. With the template approach, environments can be provisioned in seconds with consistent configuration and security.

TIP

When you step up to bat with the IT automation capabilities of NSX Data Center, you're poised for a triple play:

- Reduce operational expense.
- Accelerate time to market.
- Speed IT service delivery.

Developer cloud

NSX Data Center is ideally suited for use as a platform for self-service developer clouds, as well as other Infrastructure-as-a-Service (IaaS) initiatives. You can use automated network and service provisioning to give your development and test teams fast access to the infrastructure they need — so they can get software apps and upgrades into the hands of users in less time.

NSX Data Center can provision thousands of isolated networks for development, testing, and staging environments — all on the same physical infrastructure. In this new way of doing business, NSX Data Center removes the manual tasks and cycle time associated with procuring, installing, and configuring network infrastructure. Networks are deployed in lockstep with their workloads — as fully audited self-service transactions. Applications quickly move through development, testing, staging, and production without changes to their IP addresses.

Multitenant infrastructure

Thanks to virtualization, provisioning network infrastructure for development/testing teams is no longer a bottleneck that slows down the business and delays time to market.

In multitenant cloud environments, you can use the micro-segmentation and isolation capabilities of NSX Data Center to

maintain isolation between tenants. NSX Data Center enables you to create virtual networks and have them completely isolated from any other virtual network and from the underlying physical network. You can have two different tenants running on the same IP addresses on the same physical infrastructure without having any conflict between these IP addresses because the virtual networks don't even know that the other exists, nor do they know that the physical network exists.

For a broader solution, you can add advanced services based on virtual network, network segment, or security group. For example, you might add deep packet inspection via firewalls such as those from Palo Alto Networks. With this service, you can granularly define traffic flows that will be redirected to the Palo Alto Networks VM-Series firewall for inspection and enforcement. Traffic allowed by the VM-Series Firewall is then returned to the NSX Data Center virtual switch for delivery to the final destination (guest VM or physical device).

Cloud-native applications

Developers are increasingly going over the heads of IT and building apps in the cloud. They're using new constructs like containers, building apps using microservices architectures, and using container orchestration platforms to build and scale out their applications. Organizations are grappling with ways to insert some level of visibility and control in this process, without slowing the development teams down or giving them hoops to jump through that they most likely will simply ignore.

NSX Data Center taps directly into application and container orchestration platforms like Kubernetes or Cloud Foundry in order to provide visibility in this realm to the broader organization and apply policies already in NSX Data Center into the container domain. This allows organizations to help development debug to the container level when something in a product application goes wrong. It also allows business-centric policies — for example, PCI compliance for payment transactions — to be applied within the application, inherently picked up from developers' manifests as applications are built.

Multi-Cloud Networking

According to RightScale's 2018 "State of the Cloud Report," on average, organizations leverage five different clouds. *Five.* Even organizations that are not using public clouds due to regulatory issues still manage multiple private data center clouds (private clouds) to improve application continuity and keep the business running. Organizations that do use public clouds may have one developer spinning up an app in Amazon Web Services (AWS) while another is doing so in Google Cloud Platform. Meanwhile, a whole separate team may have a complete project in Microsoft Azure.

Managing IT processes, planning for disasters, ensuring security, all across multiple private data centers and/or public clouds is now a business must. The good news is that network virtualization makes this possible and removes barriers that used to present challenges here. By extending the network across clouds, and by managing security in one place across clouds, cross-cloud networking and security becomes both technically possible and operationally feasible.

Disaster recovery

The recovery process is automated, orchestrated, and fully integrated across compute, storage, networking, and security. NSX Data Center is compatible with several disaster recovery (DR) orchestration tools, such as VMware Site Recovery Manager, Dell EMC RP4VM, Zerto, and Veeam.

NSX Data Center provides consistent logical networking and security across protected and recovery sites, which lowers the recovery time objective (RTO) in the event of a disaster. With networks and security spanning consistently multiple sites, applications can recover in the recovery site and retain their network and security configurations.

In addition, NSX Data Center can be used to easily create test networks that can be used when testing recovery plans without disrupting the production environment. The testing occurs in an isolated environment, and maintains the same application IP addresses and security policies at the recovery site.

Metro pooling and data center extension

Multi-site pooling creates a unified, seamless, and resilient pool of infrastructure to run applications across multiple data centers and to the cloud, enabled by a single consistent networking platform. In the same way, apps can be deployed in any location and connect to resources located across sites to accommodate disaster avoidance, planned and unplanned outages, or better resource utilization.

Additionally, the increased mobility of workloads over a common network means that downtime can be planned more efficiently and that scaling existing data centers or bringing new ones online or integrating new ones from mergers and acquisitions is significantly simplified. This has been a prevalent use case for NSX Data Center in multi-site deployments.

Consistent security across clouds

After the network is virtualized, extending its benefits to the cloud becomes a simple add-on. VMware NSX Cloud does exactly this by adding native cloud workloads to the foundation of VMware NSX Data Center, using one management portal for workloads on premises and in the cloud. This enables micro-segmentation over east–west traffic between application workloads running in the cloud or in the private data center.

You can now define a security policy once and apply it to workloads anywhere — across cloud virtual networks, regions, availability zones, and multiple private data centers and public clouds. Security policies are dynamically applied based on workload attributes and enforced at the instance level. Security rules follow workloads when they're moved. You can define policies based on rich constructs, such as workload attributes and user-defined tags. You can also do things like respond to threats gracefully with a quarantine of rogue or compromised cloud endpoints.

IN THIS CHAPTER

- Introducing the concept of operationalizing
- Walking through a network virtualization deployment use case
- Addressing issues related to staffing and jobs

Chapter 5
Operationalizing Network Virtualization

Operationalizing network virtualization involves optimizing people, processes, and technology to maximize the network and the security capabilities it enables.

Your enterprise must be successful at operationalizing network virtualization to achieve the overarching benefits of speed, agility, and security. How well you operationalize network virtualization will determine how fast you realize measureable IT and business benefits — the ultimate prize.

Operationalizing network virtualization should be viewed as a gradual cultural and technical journey, where your organization achieves ever-growing maturity and sophistication as you move from a hardware-defined data center to a software-defined data center (SDDC). It's a journey that will make heroes and careers, just as compute virtualization did a decade ago.

The purpose of this chapter is not to provide all the answers to what it takes to operationalize NSX Data Center (which would take a book in itself), but rather to introduce the topic and highlight some of the key areas you should consider on your journey to network virtualization.

TIP

As you embark on your network virtualization journey, clearly define your long-term vision for your fully optimized SDDC. Consider how you need to evolve your people, processes, and tooling to get you there.

Investigating Operations Investment Areas

You should consider three key operations investment areas on your journey toward network virtualization. These investments help you gain maximum business value for your organization and maximum career value for your IT staff.

Take a holistic approach, one that encompasses these concepts, each of which is covered in detail in the following sections:

- People
- Process
- Tooling

People and process

SDDC operations impact most of the IT organization. These operations span compute, networking, storage, security, and personnel — including operators, administrators, engineers, and architects.

TIP

When you operationalize network virtualization, include all necessary players in the process — and be transparent.

Here are some other best practices regarding your IT organization and its people:

- **Your existing network and security teams take on NSX Data Center.** There's no need to change your teams or create new ones. Functional roles also remain the same (for example, architects, engineers, operators, admins). Existing roles and responsibilities evolve to include network virtualization.

- **Consider how you can create a more blended cloud team** with cross-domain and cross-disciplinary skills, common goals and operating principles, intra-team training and development, and alignment around service delivery for the business.
- **Consider these networking and security roles for your cloud network:** Architecture, security, orchestration and automation, development and integration, administration, operations, and support and escalation.
- **Garner your team's support.** Make sure all players on your team understand the value proposition and what it will mean to them personally and professionally as new opportunities to work on more interesting and strategic projects become available.
- **Reassure your networking staff about their job security.** Make it clear to your networking staff that they will not be automated out of jobs and that their jobs will not be moved to the virtualization team. Your existing networking staff takes on network virtualization. Only they have the required networking expertise.
- **Involve your cloud operations staff early in the evaluation process.** That way, they can learn how NSX Data Center will make their jobs easier, and they can become advocates for the project. Don't surprise them just before you want to deploy.
- **Include security early in the evaluation.** The security team needs to learn how isolated virtual networks are as secure as physical networks. They need to learn that micro-segmentation does not replace existing perimeter firewalls for north–south traffic, but rather allows your organization to control east–west traffic inside the data center.

TIP

Take advantage of VMware's operations-focused resources (technical guides, workshops, training, and certifications) to gain the necessary expertise, skills, and knowledge required for network virtualization and the SDDC.

Processes and tooling

One primary benefit of network virtualization is that formerly manual processes can be automated. This does, however, require some upfront investment in the appropriate tools. Some

automation of tasks can be achieved directly within the NSX Manager, whereas other automation functions will be provided by other tools, such as a cloud management platform.

NSX Data Center provides a central point of control — the NSX Manager — for the creation, management, and monitoring of virtual networks. Operation of an NSX Data Center environment will naturally focus on the NSX Manager, either through its user interface (UI) or via application programming interface (API) calls made to the NSX Manager by other tools (such as VMware vRealize Automation, VMware vRealize Operations, OpenStack, and other third-party tools).

In addition, managing the underlying infrastructure, which includes both NSX Data Center components (controllers, edge nodes, hypervisors) and network infrastructure (the underlay), will be necessary. NSX Data Center provides its own capability to manage these elements, and third-party tools may also play a central role in managing the infrastructure.

TIP

When you operationalize network virtualization, take a step back and consider the full range of implications for your processes and tooling. In particular, keep these best practices in mind:

- **Analyze your existing network and security processes, and understand them in detail.** Determine how to simplify and streamline your processes via orchestration and automation.
- **Consider the impact that network virtualization has on activities such as monitoring, troubleshooting, change management, release management, and capacity management.** Understand how these key activities work today and how they can be simplified.
- **Determine your priorities for automating networking processes and standardizing environments (for example, configurations and policies) to reduce operational effort and expenses.** Automation and policy-based provisioning of networks and services eliminate common configuration errors and improve tracking of changes for audit and compliance.
- **Determine whether you should use your existing management and operations tools or whether you should evaluate modern alternatives.** These modern

alternatives provide an end-to-end view of application health across compute, storage, and networking. Gain visibility into the object relationships between virtual and physical components.

- **Identify VMware and third-party tools for management of virtual and physical components.** Assess how you can leverage NSX Data Center native capabilities and APIs for deep integration with existing tools, such as cloud management platforms and orchestration and automation tools.
- **Use your existing tools to operate virtual networks.** Virtual networks provide all the operational information that is expected from physical networks (for example, packet and byte counters, NetFlow export). Many existing tools can leverage the information provided by NSX Data Center for operational tasks.
- **Use your existing favorite tools to monitor and troubleshoot.** A single-vendor approach doesn't always give you the best visibility. You may find that using multiple tools (for example, vRealize Network Insight, vRealize Operations, Splunk, Wireshark, or NetFlow collectors) will allow you to best monitor and troubleshoot your network infrastructure.

Looking at Some Examples

There are a number of things you can use network virtualization for. For illustrative purposes, this section walks through three examples of current state versus ideal state made possible by network virtualization.

Provisioning and configuration management

Virtualized infrastructure and APIs bring automation to provisioning, configuration management, and compliance tools.

Current state

- Rack and stack physical devices and manually configure them through command-line interfaces (CLIs) or scripts.
- Ticketing systems (for example, Service Now) generate multiple requests and track status.

- Network configuration management (NCM), configuration management database (CMDB; for example, HPNA), and compliance tools track configuration items and their relationships.

Ideal state

- Orchestration/cloud management platform (CMP) tools (for example, vRealize Automation, Chef, or Puppet) provide automation for provisioning and configuration management.
- Self-service portals provide catalogues of services and automation with APIs.
- Standardized templates include built-in relationships. You can leverage APIs to discover the topology and check configuration assurance through external tools.

Incident and capacity management

Monitoring, troubleshooting, and capacity management are delivered through application-aware and virtual plus physical context tools.

Current state

- Siloed monitoring and troubleshooting tools focus on physical infrastructure.
- Multiple tools consume different granularity of information without correlation.
- Centralized Manager of Managers (MoMs) tied with ticketing systems generate automated alerts.

Ideal state

- Application-level monitoring, troubleshooting, and capacity management span domains and virtual and physical infrastructure.
- A simplified user interface provides a unified and correlated view of SDDC infrastructure.
- Auto remediation is provided through external monitoring tools using an API framework. Scale-out of NSX Data Center capacity is based on utilization.

Micro-segmentation

This security technique enables fine-grained security policies to be assigned to applications, down to the workload level.

Current state

From a practical standpoint, micro-segmentation is feasible only when a data center is using a virtualized, software-only approach.

Ideal state

- Understand network traffic with application-level monitoring (for example, VMware vRealize Network Insight) to automate a traditionally manual and labor-intensive process of identifying what applications are communicating with each other.
- Implement firewall rules after you've selected the target application (for example, by using NSX Data Center's built-in Application Rule Manager).
- Continue to monitor network traffic and troubleshoot across your entire environment (for example, vRealize Network Insight, VMware vRealize Log Insight, and NSX Data Center built-in tools: Flow Monitoring and Endpoint Monitoring). Repeat with the next application.

Developing the Right Mind-Set

Change isn't easy — especially when it involves something personal. Unfortunately, though, it happens whether we like it or not. In the world of information technology, change is upon us. *IT automation*, *micro-segmentation*, *application availability*, and *cross-cloud services* are no longer buzzwords in marketing materials and executive meetings. These are realities designed and deployed in some of the world's largest IT environments. The common thread among these concepts is the new capabilities in networking and security brought to life by the NSX family.

Network virtualization is transforming the way enterprises approach traditional business problems, and it's solving new business problems brought about by a company's digital transformation.

As an IT professional, your long-term success hinges on your ability to adapt to new technologies and solutions. NSX solutions are disruptive to the status quo, but at the same time it's an opportunity for your admins, engineers, and architects to become leaders in a new paradigm of networking and security. This requires a mind-set focused on finding opportunities rather than believing your abilities are fixed.

Ready to take your career to the next level? Check out Chapter 6 to learn how.

Focusing on the Big Picture

Like any major IT initiative, network virtualization changes a lot of things in your data center. But one thing it doesn't change is your job security. Networking pros are essential to the success of a virtualized network environment. You can't get there without them.

When you're part of a network virtualization initiative, you have the opportunity to participate in and contribute to the transformation of networking and security at your company. The outcome will be beneficial for you, just as it was for those who championed and built their careers on compute virtualization. Embrace this important leadership opportunity.


TIP

As you virtualize and automate your infrastructure, you'll be free to work on more interesting and strategic initiatives. For example, instead of spending your time on the mundane work of configuring a router or updating firewall rules, you can work on designing a spine-leaf network, automating networking and security workflows, or perhaps building a developer cloud.

Participating in a network virtualization initiative will enrich you professionally, prepare you for the future, and make you more valuable in the job market — just as server virtualization did for server admins a decade ago.

REMEMBER

Network virtualization advances your career, allowing you to spend more time on network architecture, design, and traffic engineering:

- **When you implement network virtualization, you won't be automated out of a job.** Instead, your job will be transformed to allow you to work on more interesting and strategic projects.
- **Your job won't go to the virtualization team.** NSX Data Center relies on the same networking concepts and technologies as physical networks, so it requires networking and security expertise.
- **Virtualization won't make your job more difficult.** The virtual overlay, combined with automation and a simplified physical underlay, streamlines network provisioning and management.

If you'd like to learn more about operationalizing network virtualization, check out the library of NSX Day 1 resources at `www.vmware.com/go/runnsx`.

IN THIS CHAPTER

- Highlighting resources packed with valuable insights
- Test-driving with NSX Data Center
- Deploying NSX Data Center into your environment

Chapter 6
Ten (Or So) Ways to Get Started with Network Virtualization

This chapter tells you what you've always wanted to know about getting started with network virtualization but were afraid to ask. Here, we provide a library of resources on network virtualization, highlight opportunities to deploy the VMware NSX Data Center platform with Cisco infrastructure, and explain how NSX Data Center is designed for integration with your existing infrastructure and third-party solutions for network services, such as load-balancing devices and next-generation firewalls.

The chapter starts with a look at some of the resources that are available to help you enrich your understanding of network virtualization, the components of a virtualized network, and the tools that are available to help you get started.

Boning Up on the Basics

VMware offers a wide range of resources to help you get grounded in the basics of network virtualization:

- **VMware NSX Data Center Introduction Video** (`https://youtu.be/gqcwJEhIiqs`): This fast-paced three-minute video explains how NSX Data Center serves as the foundation for a network virtualization platform that delivers the operational model of a virtual machine.
- **The VMware NSX Data Center product page** (`www.vmware.com/go/nsx`): The NSX Data Center product page summarizes the basic features, functions, and benefits of the NSX Data Center platform. It also serves as a portal that provides links to a wide range of deep-dive assets, including technical information and business-focused content.
- **VMware NSX YouTube channel** (`www.youtube.com/vmwarensx`): The NSX YouTube channel provides a wide variety of videos — animated overviews, customer stories, short lightboard walkthroughs, product deep dives, and more.
- ***Micro-segmentation For Dummies*** (`http://learn.vmware.com/41021_REG`): This e-book, provides a close-up look at the micro-segmentation use case for network virtualization, including the basics on how it works, the enabling technologies, and the wide-ranging security benefits. Learn how to develop an inherently secure data center that helps prevent the lateral spread of attacks within your data center.

Taking a Deeper Dive

VMware also offers a wide variety of technical resources to help you understand what's going on "under the hood":

- **VMware NSX Data Center for vSphere Network Virtualization Design Guide** (`https://communities.vmware.com/docs/DOC-27683`): For the truly deep-dive technical stuff, download the design guide. This document is targeted toward virtualization and network architects

interested in deploying the NSX Data Center network virtualization solution in a vSphere environment. This guide includes detailed information on NSX Data Center for vSphere functional components, functional services, and design considerations.

- **Getting Started Guide for NSX Data Center for vSphere** (`https://communities.vmware.com/docs/DOC-27705`): This resource provides step-by-step examples that demonstrate how to set up network services in NSX Data Center for vSphere, including the following:
  - Logical switches
  - Logical distributed routers
  - Distributed firewalls
  - Logical centralized routers (edge) with dynamic routing and with many-to-one network address translation (NAT)
  - Logical load balancers (edge)
- **VMware NSX-T Data Center Reference Design Guide** (`https://communities.vmware.com/docs/DOC-37591`): This design guide does not assume familiarity with NSX Data Center for vSphere, and it treats knowledge of the platform independently. This guide includes detailed information on bare-metal edge node deployments and cluster design, covering multi-vCenters ESXi deployments (including kernel-based virtual machine [KVM]–only designs).
- **VMware Press NSX Data Center Day 1 and Day 2 Guides** (`www.vmware.com/go/runnsx`): Our experts have published e-books on essential network and security topics to help you get started with NSX Data Center:
  - *NSX Micro-segmentation Day 1*
  - *NSX Micro-segmentation Day 2*
  - *Building VMware NSX Powered Clouds and Data Centers for Small and Medium Business*
  - *Operationalizing VMware NSX*
  - *Automating NSX for vSphere with PowerNSX*

  New e-books are published quarterly, so check back periodically for new topics.

- **The Network Virtualization blog** (`http://blogs.vmware.com/networkvirtualization`): Check out this blog for everything from the latest news to deep technical insights and how-to tips about network virtualization. It serves as a key industry source for accurate news and factual information about network virtualization.

Taking an NSX Data Center Test Drive with Hands-On Labs

To enrich your understanding of a platform like NSX Data Center, it always helps to hop into the driver's seat for a test drive:

- **VMware NSX Hands-on Lab** (`www.vmware.com/products/nsx/nsx-hol.html`): VMware Hands-on Labs deliver a fully operational live desktop environment for you to experience VMware products with no setup required. With click-by-click guidance and all products preinstalled, you can focus on the product features you value most. This is a great way to get closely acquainted with the capabilities of NSX Data Center without installing any software on your system.

  Here are some example Hands-on Labs you'll find on this site:

  - VMware NSX Data Center Intro Lab
  - VMware NSX Data Center – Distributed Firewall with Micro-Segmentation
  - Intro to vRealize Network Insight
  - VMware NSX Data Center Advanced Lab
  - Horizon and NSX Data Center for Healthcare
  - Getting Started with NSX-T Data Center

Gaining Visibility

You can't protect what you can't see. Understand what applications are communicating with each other with the Virtual Network Assessment (VNA, `www.vmware.com/go/vna-field`), which

leverages the VMware Network Insight product. Get insights within 24 hours. The VNA will

- Show your network traffic distribution by type (east–west, Internet, routed, VM to VM) and by services (web, database, mid-tier, infrastructure).
- Provide a preview of actionable NSX Data Center micro-segmentation recommendations for your network.
- Highlight your opportunities to optimize network performance with NSX Data Center.

Discovering How to Deploy NSX Data Center in Your Environment

When you're ready to explore your deployment options, you can get started by learning about network virtualization and NSX Data Center via on-demand resources. VMware offers a variety of ways to experience the benefits of network virtualization and NSX Data Center, from online courses to live webinars to self-paced on-demand courses.

Start your journey by learning about the fundamentals of network virtualization and the business challenges NSX Data Center can help you solve. After that, you can take a self-paced, on-demand course that provides a sneak peek into how to install, configure, and manage NSX Data Center. To learn more, check out the following:

- **Coursera (free;** `http://vmware.com/go/coursera`**):** Continue your education with "Networking and Security Architecture with VMware NSX" on Coursera. This free online course equips learners with information on basic networking virtualization with VMware NSX Data Center. To get the most of this course, you should have familiarity with generic IT concepts of routing, switching, firewalling, disaster recovery, business continuity, cloud, and security.

- **Network Virtualization Fundamentals** (`https://mylearn.vmware.com/mgrreg/courses.cfm?a=det&id_course=240782&ui=www_edu`): Get started with a three-hour self-paced online course that will provide you with a fundamental understanding of virtual networking and the business challenges it solves.
- **Certification in Network Virtualization** (`https://mylearn.vmware.com/mgrReg/plan.cfm?plan=48389&ui=www_edu`): Gauge your level of skill designing, implementing, and managing an NSX Data Center environment. You can find the following:
  - **VMware NSX: Install, Configure, Manage:** A five-day course in which you learn how to use logical switching and routing, gateway services, firewall configurations, and security services.
  - **VMware NSX: Design & Deploy:** A five-day course that prepares you to lead NSX Data Center design and deployment projects by giving you an understanding of general design processes and frameworks.
  - **VMware NSX: Troubleshooting and Operations:** A course in which you learn how to isolate problems and identify resolutions through a systematic process.
  - **VMware NSX for Internetworking Experts Fast Track:** A course for those who already have a Cisco Certified Internetwork Expert (CCIE) certification. You learn how NSX Data Center intersects with the virtualization functions of a Cisco-based infrastructure in spine-leaf and traditional core-aggregation-access architectures.

Deploying NSX Data Center on Your Existing Network Infrastructure

NSX Data Center is designed to run over any network hardware, and in most cases it also integrates in order to bridge the physical and virtual worlds using the level 2 gateway functionality. These integrations recognize that in the hyperdynamic environment of the modern data center, the underlay transport network and the

overlay network virtualization solutions are codependent actors in the delivery of optimal performance, reliability, and scale.

To enable these integrations, VMware works actively with its level 2 switching partners to create reference architectures and design guides for using NSX Data Center as an agile overlay that leverages the capabilities of the underlay infrastructure.

Here's a sampling of the technical resources that are available to guide the integration of NSX Data Center with your existing network infrastructure:

- **Arista:** VMware and Arista Network Virtualization Reference Design Guide for VMware vSphere Environments (`https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-arista-nsx-design-guide.pdf`)
- **Cisco 9K:** Reference Design: Deploying NSX with Cisco UCS and Nexus 9000 Infrastructure (`https://communities.vmware.com/docs/DOC-29373`)
- **Dell:** Network Virtualization with Dell Infrastructure and VMware NSX Reference Architecture (`https://communities.vmware.com/docs/DOC-27684`)
- **Juniper:** Connecting Physical and Virtual Networks with VMware NSX and Juniper Platforms (`https://communities.vmware.com/docs/DOC-27610`)

Integrating with Your Networking Services Ecosystem Partners

In addition to integrating with your existing network infrastructure, NSX Data Center is designed to integrate with solutions for various network services, such as load-balancing devices and next-generation firewalls and services:

- **Physical-to-virtual data center services:** Arista Networks, Dell EMC Open Networking, Extreme Networks, HPE, Huawei, Juniper Networks

- **Security services:** Bitdefender, CA Technologies, Check Point, ESET, Fortinet, HyTrust, Juniper Networks, Kaspersky, McAfee, Palo Alto Networks, Symantec, Trend Micro
- **Software-defined data center (SDDC) operations and visibility:** AlgoSec, Dell EMC, Firemon, ForeScout, Gigamon, NetScout, RedSeal, Riverbed, Skybox, Tufin


TIP

For an up-to-date list of VMware technology partners and resources, go to `www.vmware.com/products/nsx/technology-partners.html`.

Make network virtualization work for you

In many ways, networking is stuck in a hardwired past. With conventional approaches to the network, services still require manual provisioning and are anchored to vendor-specific hardware. This old way of doing things slows application deployment time and blocks the road to the software-defined data center. Network virtualization changes this equation. Virtualized networks are created, provisioned, and managed entirely in software, bringing new levels of agility, efficiency, and security to data center operations.

Inside...

- Learn what network virtualization is
- See how it differs from conventional network architectures
- Discover how network virtualization can help you operate more efficiently
- Understand the architecture and best practices

vmware®

Jonathan Morin has worked more than 15 years in networking, designing service provider networks and building data center and campus networking products. He received his BSCS from UNH and his MBA from UC Berkeley Haas. **Shinie Shaw** has over 5 years of experience in networking with Cisco and VMware and 10 years in regulated industries. She received her BS from Northwestern University and MBA from UC Berkeley Haas.

ISBN: 978-1-119-55049-5
Not For Resale

for dummies®
A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.