LEARNING MADE EASY

VMware 3rd Special Edition

Network Virtualization

for dummies®
A Wiley Brand

See why you need to virtualize your network

Understand how it works and getting started

Brought to you by vmware®

Varun Santosh
Stijn Vanveerdeghem

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 22 years of breakthrough innovation benefiting business and society.

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

Network Virtualization

VMware 3rd Special Edition

by Varun Santosh and Stijn Vanveerdeghem

for dummies®
A Wiley Brand

Network Virtualization For Dummies®, VMware 3rd Special Edition

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

ISBN 978-1-119-73684-4 (pbk); ISBN 978-1-119-73682-0 (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 BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

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

Project Editor: Elizabeth Kuball
Acquisitions Editor: Ashley Coffey
Editorial Manager: Rev Mengle
Business Development Representative: Karen Hattan
Production Editor: Siddique Shaik
Special Help: Faithe Wempen

Table of Contents

Introduction

Perhaps you've heard some talk about network virtualization, and wondered what it was all about. How can something physical, like network hardware, become something entirely existing in software? And how does it change the way networks operate and IT professionals do their jobs?

Welcome to *Network Virtualization For Dummies,* your guide to a new and greatly improved approach to networking and security. This book teaches you the basics of virtualization and explains how it can help a business save money, run faster, and be more secure.

Keeping up with modern business's expectations is a tall order for any network. A network needs to be

- Agile and configurable enough to move as fast as the business itself
- Smarter and faster than the cybercriminals who are always looking for a way in
- Flexible enough to enable users to run applications and access data from anywhere in the world

Network virtualization can help your company realize all those goals and more.

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.

WARNING

Anything marked with this icon will save you a load of trouble (or worse).

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 and security challenges**
- **Building the case for network virtualization**
- **Introducing the virtual cloud network**

Chapter 1
Evolving to a Modern Network

Why should you care about network virtualization? Why are organizations increasingly adopting virtualization technologies? This chapter explores several challenges that point to a single overarching need: Organizations want to deliver public cloud-like agility, flexibility, efficiency, and reliability with their private-cloud infrastructure. Here's why:

- To stay competitive, businesses need agility to speed up time to market.
- Companies face increasingly heterogenous infrastructures, from the edge to branch offices to core data centers and the cloud.
- Legacy network architectures limit business agility, leave security threats unchecked, and drive up costs.
- Using dedicated hardware for each network function prohibits an agile, scalable approach.

How Network Virtualization Is Changing Everything

Network virtualization is rewriting the rules for the way services are delivered. It decouples networking and security services from underlying network hardware by creating logical virtual networks. Organizations are taking a full-stack layer 2 to layer 7 approach with network virtualization, delivering services like virtual switching and routing, firewalling, and load balancing that are built into the infrastructure. Armed with this ability to define and consume the network in software, organizations can centrally provision the network on-demand while simplifying configuration and improving scale and resource efficiency. This approach transforms the networks from static, inflexible, and inefficient to dynamic, agile, and optimized.

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

With network virtualization enabling the software-defined data center (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, apps, and endpoints.

According to the *Flexera 2020 State of the Cloud Report,* enterprises continue to scale their multi-cloud strategies, with 87 percent of organizations having a hybrid cloud strategy. Similarly, according to the annual *CNCF Survey 2019,* the use of containers for user-facing applications increased significantly, with 84 percent of respondents using containers in production, up more than 15 percent from 2018. Network virtualization is playing a central role in simplifying connectivity and security in these heterogenous environments, enabling organizations to build and deploy these applications faster.

Today's Networking and Security Challenges

That all sounds pretty good, doesn't it? But there are quite a few technical details to work out between here and there. We'll kick things off by looking at some of the networking and IT challenges companies face today. Upcoming chapters explain how network virtualization can help solve many of them.

Businesses need speed

Organizations of all sizes are experiencing a rapid increase in the pace of change. Everything needed to be done yesterday — new innovations and feature delivery, competitive responses, and 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 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 have to ask IT.

Security requirements are rising

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. Vulnerabilities in applications are the primary targets of attackers ranging from cybercriminals to nation-state actors. Traditional firewalls alone are inadequate to protect against attacks that come in through valid channels, such as legitimately open ports. Examples of this type of attack include SQL injections and wormable ransomware leveraging exploits such as EternalBlue to laterally spread across vulnerable Server Message Block (SMB) servers within the data center.

Organizations are building security into the software development life cycle, but that has by no means eliminated unsecure code and vulnerable software. Fixing vulnerabilities after applications have been deployed is costly and leads to downtime. So, network security should be applied as close to the application as possible and the life cycle of a security policy should be directly tied to the life cycle of the application.

Apps and data are in multiple clouds

There is no longer a simple answer for where apps are running and where the data resides. Some apps start in the cloud where some developers begin to code and test. Many companies find that certain apps are best run in the private data center, both for cost efficiencies and private control. Many other organizations have moved apps away from their original deployment location — from the private data center to the public cloud to delegate management, or from the public cloud to the private data center to rein in public-cloud costs or to take advantage of new private-cloud consumption models. Today's 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 also 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.

Why Hardware-Based Networks Can't Keep Up

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. Here's a summary 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.*

Although many 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

Some network provisioning processes can be scripted — and certain software-defined networking (SDN) models promise to make this a reality. However, 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. Therefore, 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 may mean replication to an off-site 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 network hardware can interfere with that. 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. Not only is this process slow and complex, but it will eventually reach scalability limits.

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. This, in turn, puts the same limits on the business itself, because the business can move no faster than IT can move.

In its 2018 report called *Look Beyond Network Vendors for Network Innovation,* Gartner says 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:

- Data center network requests commonly 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 so 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.

A high price tag is 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."

Operational and capital expenditures 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.

CapEx

On the CapEx 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, including routing, switching, firewalling, analytics, 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 and the need to deploy active–passive configurations. In effect, you need to buy twice the hardware for high availability — 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 demand requires this inefficiency. And up goes the costs of networking.

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 have envisioned 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?

Traditional firewalls aren't adequate

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 attacks, but not all of them. As recent attacks have shown, threats are still slipping into the data center through legitimate access points. Once inside, often there is nothing in place to prevent them from spreading within the data center. This problem has been a tough one to solve because of the realities of physical network architectures. Put simply, with legacy networking systems, providing firewalling for traffic between all workloads inside the data center is too costly.

Using a traditional hardware firewall as an internal firewall in the data center requires hairpinning. Traffic needs to be sent up from a workload on the hypervisor across the network, across racks to a physical firewall, and then back again, even if both the source and the destination reside on the same hypervisor.

Even more important, inserting a traditional firewall into an existing brownfield environment requires significant re-architecture, not just of the network itself but, more critically, of the applications. Many customers start with a perimeter firewall protecting the demilitarized zone (DMZ) from the outside and the internal network from the DMZ. As organizations grow, they realize that they need to segment that internal network. Doing this with a traditional firewall means that application IP addresses would need to be reassigned. It also results in segmentation that is very rigid and limited to network constructs and VLANs.

Having a firewall policy that relies on IP addresses and ports leads to delays, forcing customers to adopt very coarse security policies that often become stale and remain in place long after an application has been decommissioned.

As new applications are brought up and legacy applications are decomissioned, firewall policies need to be updated very frequently, and the policies consist of much larger rule sets than at the perimeter. Traditional firewalls don't have the software-defined architecture that enables them to scale with the massive

amount of traffic, large rule bases, and constant policy updates that are required on the internal network.

REMEMBER

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
- Comparing network virtualization and software-defined networking
- Looking at the differences between virtual appliances and virtual layer integration
- Seeing why now is the time for network virtualization
- Thinking of the network in new ways

Chapter 2
Virtualizing 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.

Understanding How Network Virtualization Works

Network virtualization makes it possible to programmatically create, provision, and manage networks completely within 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). They're attached to individual workloads, such as 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.

Just as a VM or a container is a software construct that presents logical services to an application, a *virtual network* is 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 enables the entire network to be created in software (see Figure 2-1).

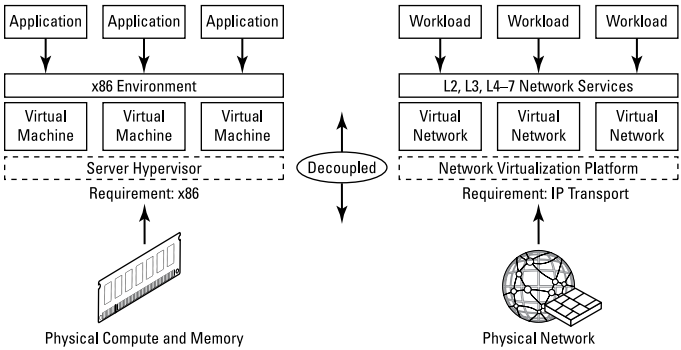

FIGURE 2-1: Compute and network virtualization.

Network virtualization coordinates the virtual switches across the various environments (such as hypervisors and clouds) along with the network services (such as firewalling and load balancing) to effectively deliver a networking platform and create dynamic virtual networks.

Another advantage of network virtualization is that you can provision network resources and services through a number of interfaces. One set of options makes use of the native user interfaces such as 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. 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 2-2).

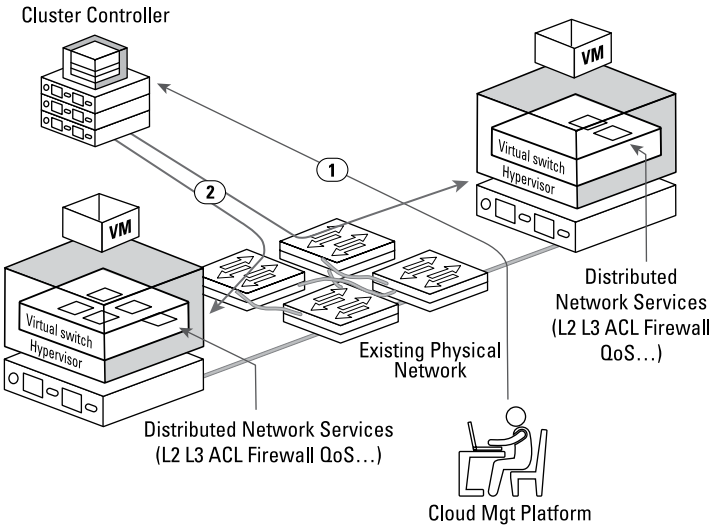

FIGURE 2-2: Virtual network provisioning.

This flexibility not only allows different virtual networks to be associated with different workloads in the same environment (such as cluster, pod, hypervisor, application instance, and 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. Workloads see the same layer 2 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.

To the physical network, a virtual network looks and operates like a traditional physical network (see Figure 2-3). 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).

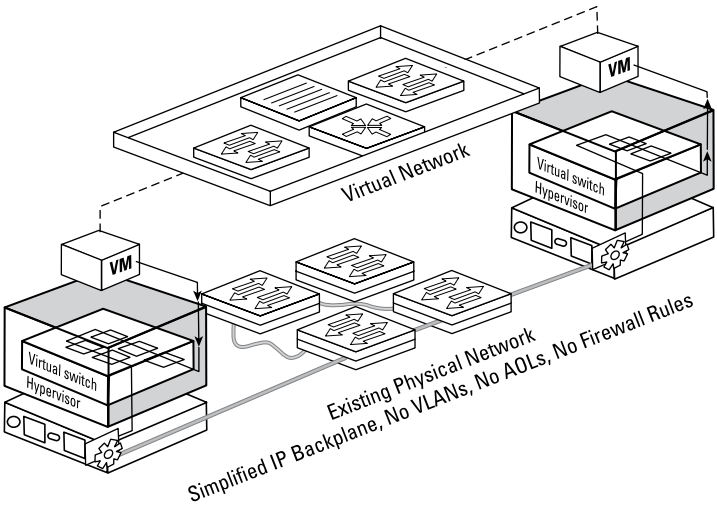

FIGURE 2-3: The virtual network, from the network's perspective (physical).

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

Differentiating Between 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.

Software-defined networking makes the network more agile by defining networking constructs in software. In this regard, network virtualization and SDN are similar.

How SDN manifests varies widely. In some instances, the goal is to manage physical network device configuration. In others, it's about broadly orchestrating the network services by tying multiple systems together via application programming interfaces (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. It completely decouples network resources from the underlying hardware, with networking components and functions 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.

Comparing Virtual Appliances to Network Virtualization

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.

Network virtualization integrated 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.

Understanding Why the Time Is Right for Network Virtualization

People have been talking about network virtualization for years. It's 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.

Redefining security with micro-segmentation

Network security has traditionally been built around unchanging network topology. Back in the day, applications were static and typically confined to one environment. Organizations achieved a

degree of segmentation by using a network-based security policy with a firewall filtering traffic crossing a VLAN.

Today however, the reality is different. Applications are deployed across hybrid environments, so they may not be fully visible to the infrastructure administrator tasked with ensuring proper application security enforcement. At the same time, automation-driven application deployment models and continuously changing applications have resulted in infrastructure and security teams having to continuously redefine networking and security configuration.

All too often, infrastructure teams and application owners/developers don't speak the same language. Application owners lack proper tools to effectively determine and communicate networking and security requirements for applications they develop, leading to long delays in application rollouts and sometimes incorrectly configured policies.

With applications continuously changing and moving across hybrid clouds, a security policy based on static constructs like VLANs or subnets is inadequate and hard to maintain, and leads to an ever-expanding set of firewall rules even long after applications have been decommissioned.

An attacker's initial target is almost never his ultimate objective. After an attacker has gained access, lateral movement is frequently an intermediary step along the way to the crown jewels. A firewall deployed between network segments has no means of controlling or even providing visibility of lateral spread within a segment.

All these challenges lead to operational inefficiencies and unmitigated risk, making the jobs of both application owners and infrastructure administrators increasingly difficult.

The NSX Service — defined Firewall enables all levels of segmentation independent of the network. This includes, for example, segmenting development and production workloads, or micro-segmenting the intra-application flows, without having to make any changes to the existing network architecture.

The distributed firewall logically sits at the virtual network interface card (vNIC) of every workload. There is no need for any hairpinning of traffic to a traditional firewall appliance, as the

distributed firewall takes action before the traffic even hits the network. This distributed architecture also means the Service-defined Firewall provides absolute coverage, with the ability to filter traffic from every workload to every other workload. The distributed firewall scales linearly with the workloads. As your organization grows and you deploy additional workload and hypervisors, you get additional firewall capacity, with line-rate throughput at every hypervisor. Network re-architecture and re-IPing are not required.

NSX Intelligence provides distributed visibility and analytics, as well as automated policy formulation for customers who are micro-segmenting their applications.

Dynamic grouping in NSX effectively ties the life cycle of a security policy directly to the life cycle of an application. Workloads are tagged to identify the application they belong to, the environment they're deployed in, whether they have any compliance requirements, and so on.

Based on these tags, workloads become members of security groups, which apply appropriate policies. When an application needs to scale up, those same tags are applied to new workloads being deployed, and the policy automatically extends to these workloads. Similarly, when an application is decommissioned, the VM is removed, or the tags are removed, the policy in the data plane automatically adjusts to reflect this new reality without any manual changes to the rule set.

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.

Rethinking the Network

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.

Although it leverages your existing network hardware, network virtualization is a fundamentally new approach to networking.

A virtualized network should enable 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

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.

IN THIS CHAPTER

- Explaining the key functions of a virtualized network
- Outlining the key features of a virtualized network
- Exploring the functional and economic benefits of VMware NSX Data Center

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.

Understanding the Key Functionalities of a Virtualized Network

A virtualized network includes both overlay networking and the traditional functions you're probably more familiar with, like routing and load balancing. Traditional networking functions, done in software, become closer to the application.

Overlay networks

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

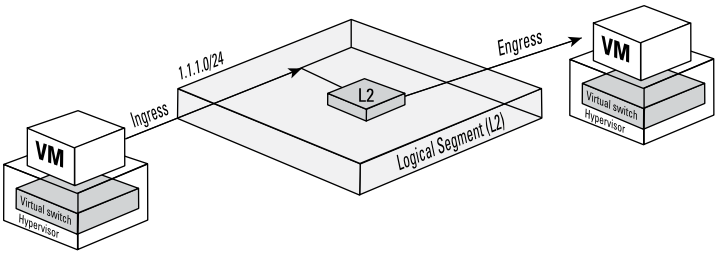

FIGURE 3-1: Logical networking via the use of overlays.

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

Virtual networks use the underlying physical network as the packet-forwarding backplane and bring nuanced networking decisions closer to the application. When application endpoints — for example, two virtual machines (VMs) — communicate, the packet is encapsulated with the IP address of the destination virtual endpoint. The physical network delivers the frame to the destination host, which removes the outer header, and then the local virtual switch instance delivers the frame to the destination.

Communication uses the underlying physical network as a simple IP backplane — without the complexity of Spanning Tree Protocol (STP) or access control lists (ACLs), because these things now can be done closer to the application by the network virtualization platform. This approach dramatically simplifies configuration management and eliminates physical network changes from.

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 other overlay technologies, too, including network virtualization using generic routing encapsulation (NVGRE). NVGRE has had limited adoption in comparison to the momentum of GENEVE and VXLAN.

Comparing GENEVE and VXLAN

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

Encapsulation

GENEVE and VXLAN both encapsulate the original Ethernet frames generated by workloads (virtual or physical) connected to the same layer 2 segment, usually named a *logical segment.* They're also both layer 2 over layer 3 encapsulation technologies. The Ethernet frame generated by a workload is encapsulated with an external header, followed by the User Datagram Protocol (UDP), IP, and Ethernet headers, and transported across the network interconnecting the GENEVE or VXLAN 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 using a 24-bit identifier, named a *virtual network identifier* (VNI) in GENEVE, or a *VXLAN network identifier* in VXLAN, 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 segment).

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. 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: increasing the maximum transmission unit (MTU) size to a minimum of 1,700 bytes. The MTU for the virtual switch uplinks of the tunnel endpoints performing the GENEVE or VXLAN encapsulation is automatically increased when preparing the tunnel endpoint.

Figure 3-2 describes the steps required to establish layer 2 communications between application endpoints leveraging overlay functionality — in this case, GENEVE:

1. VM1 originates a frame destined to VM2, which is on the same layer 2 logical segment.
2. The source Tunnel Endpoint identifies the destination Tunnel Endpoint where VM2 is connected and encapsulates the frame before sending it to the transport network.
3. The transport network is only required to provide IP connectivity between the source and destination Tunnel Endpoints.
4. The destination Tunnel Endpoint receives the GENEVE frame, de-encapsulates it, and identifies the layer 2 segment.
5. The frame is delivered to VM2.

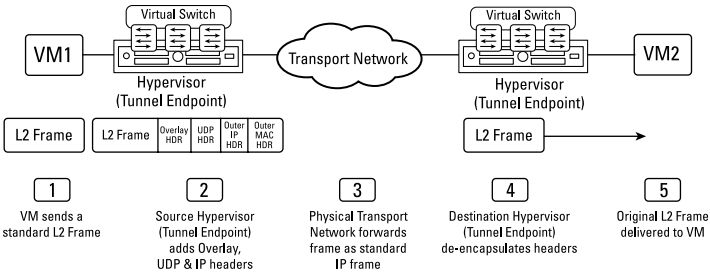

FIGURE 3-2: Establishing layer 2 communication between VMs with GENEVE.

NETWORK VIRTUALIZATION IN ACTION

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*. It adds complexity and latency, lowering performance and increasing instability, and makes it harder for application endpoints to move. By contrast, when network services are integrated into a network virtualization layer, there's no hairpinning.

Understanding Virtual Network Functions

Overlay networking is pretty powerful, but it's only one piece of the network virtualization story. Overlays enable you to make networking decisions in software, in a virtual layer, abstracted from the physical hardware. But then what? What do those decisions look like? That's where virtual network functions come in.

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.

Virtual Network Functions is a key term in Network Function Virtualization (NFV). This realm is focused on virtualizing the network functions required by service provider networks and mobile carriers. In fact, it's very similar to how functions are moving into software in the data center space, but it's also still

distinct in many ways, so it's worth clarifying that we're not necessarily talking about NFV here.

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. Network virtualization helps you

- Reduce network provisioning time from weeks to minutes.
- Achieve greater operational efficiency through automation.
- Place and move workloads independent of physical topology.
- Improve network security within the data center.

Meeting the VMware NSX Data Center

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 — to be created and provisioned in seconds. It delivers all the goodness of network virtualization that we've covered so far, and more.

In addition to increasing agility, NSX Data Center enhances security inside the data center via automated fine-grain 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 propagation. With NSX, workloads can be isolated from each other, as though each were on its own network.

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 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 endpoint independently of the underlying network hardware or topology. Workloads can be added or moved on the fly and all the network and security services attached to the app move with it. Existing applications operate unmodified because they see no difference between a virtual and 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 it 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 can virtualize portions of your network by simply adding hypervisors, bare-metal hosts, or clouds to the NSX platform.

Simplified networking

After NSX Data Center is deployed, little interaction with the physical network is required. VLANs, ACLs, spanning trees, complex firewall rules, convoluted hairpinning traffic patterns — these are no longer necessary.


REMEMBER

As you deploy NSX, you can streamline your physical network configuration and design. Vendor lock-in becomes a thing of the past with the physical network only delivering reliable high-speed packet forwarding. You can mix and match hardware from different product lines and vendors.

Broader networking and security capabilities

NSX Data Center is extremely flexible and highly extensible. A powerful traffic-steering capability referred to as *Network Introspection* allows any combination of network and security services to be chained together in any order.

Through Network Introspection, NSX provides deep integration with partners, providing the following benefits:

- **Granular service insertion:** Interception of traffic at every virtual network interface card (vNIC) or logical router uplink and flexible redirection rules
- **Simplified provisioning:** Automated deployment and plumbing of partner services, multiple deployment models, failure detection, load distribution, and failure detection
- **Ubiquitous application-based policies:** Sharing of NSX groups with partner managers, enabling a consistent application-centric partner policy with dynamically updated groups across virtual and physical appliances
- **Flexible and scalable service chain:** Chaining of multiple partner services in any combination across security and visibility, and the ability to scale up services

Both north–south and east–west Network Introspection are supported. Although north–south introspection enables the interception of the traffic at the uplink of a T0/T1 logical router, east–west introspection applies classification and interception of traffic right at the vNIC of every workload, providing the same granularity as the native distributed firewall.

This degree of flexibility applies not only to native NSX services but also to a wide variety of compatible third-party solutions — including next-generation firewalls and traffic aggregation or network/security visibility and analytics solutions.

Exploring Key NSX Capabilities

In this section, we look at some of the key technical capabilities of VMware NSX. Keep in mind: NSX virtualizes all network

functions. In addition, many that we cover, and many that we don't, are also available from the ecosystem of partners.

Everything in software

REMEMBER

Here are some of the key features of VMware NSX:

- **Logical distributed switching:** NSX allows you to reproduce complete layer 2 and layer 3 switching in a virtual environment, decoupled from 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.
- **Service-defined Firewall:** The VMware Service-defined Firewall is a distributed, scale-out internal firewall that protects all east–west traffic with security intrinsic to the infrastructure, radically simplifying the deployment model.
- **Distributed IDS/IPS:** NSX provides a software-based IDS/IPS solution that enables you to achieve regulatory compliance, create virtual zones, and detect lateral movement of threats on east–west traffic.
- **Logical load balancer:** NSX provides a full-featured advanced load balancer that delivers multi-cloud load balancing, application security, and scalable container ingress and analytics.
- **Logical virtual private network (VPN):** NSX Data Center supports site-to-site and remote access VPNs in software.
- **NSX application programming interface (API):** RESTful API enables integration with 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 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.
- **Federation, multi-site, multi-cloud networking and security:** You can extend these concepts outside a single data center domain to multiple sites and clouds.

- **NSX Intelligence:** The distributed analytics engine leverages granular workload and network context unique to NSX to deliver converged security policy management, analytics, and compliance with data-center-wide visibility.

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 perimeter protection is an essential part of a security strategy, it doesn't do everything you need. You need a new model for data center security.

NSX Data Center brings security inside the data center with automated fine-grain policies tied to application endpoints. Network security policies are enforced by firewalling controls integrated into the virtual layer. The hypervisor serves as an ideal place to enforce such policies — it's close to, yet isolated from, the application. Security policies and firewall state move when VMs move and adapt dynamically to changes in your data center, such as applications that are scaling up or being decommissioned. With NSX dynamic security groups, the life cycle of a security policy is tied directly to the life cycle of the application.

Virtual networks can operate in their own address spaces or have overlapping or duplicate address spaces. They are inherently isolated from all other virtual networks and the underlying physical network. Malicious software that slips through your firewall is no longer free to jump from server to server.

REMEMBER

An internal firewall must be able to support

- Distributed and granular enforcement of security policies
- Scalability and throughput to handle large volumes of traffic
- A low impact on network and server infrastructure
- Intra-application visibility
- Workload mobility and automatic policy management

Performance and scale

NSX Data Center delivers proven performance and scale. Because networking functions are embedded in the virtual layer, NSX

features a scale-out architecture that enables seamless scaling of additional capacity with solid availability and reliability.

Here's an example of the extreme scalability: In a real-world NSX deployment, a single cluster of controllers delivered more than 10,000 virtual networks, supporting more than 100,000 VMs. This isn't required for most networks, but many networks do have scalability limitations.

TECHNICAL STUFF

In the NSX Data Center environment:

- The processing required for distributed network services is incremental to what the vSwitch is already doing for connected workloads.
- The vSwitch is integrated with the hypervisor kernel, along with all the NSX network and security services.
- Virtual network transport capacity scales linearly (alongside application endpoint or VM capacity) with the introduction of each new hypervisor/host.

Unparalleled network visibility

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

By contrast, NSX provides all configuration and state information in one place. Connectivity status and logs for all NSX 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 single pane of glass view of the network is further enhanced with group and traffic flow visualization in NSX Intelligence, which simplifies security policy formulation across the data center.

REMEMBER

Better yet, with NSX, you have access to advanced troubleshooting tools like Traceflow. This function injects a synthetic packet into a virtual switch port, providing network path visibility as it traverses physical and logical network systems. You can identify the full path a packet takes and troubleshoot any points along the way where the packet is dropped.

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.

Identifying 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. We break the story into two groups: 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 security, that you can use to create isolated virtual network topologies in seconds.
- **Minimizing the risk and impact of data breaches:** You can use NSX 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.
- **Supporting modern applications with a converged platform:** Modern applications use a variety of compute (VMs, containers, and bare-metal). With full-stack layer 2 to layer 7 network virtualization, NSX helps you eliminate network silos, achieve consistent policy that adapts with the changing application landscape, and simplify operations.
- **Speeding up IT service delivery and time to market:** You can reduce the time required to provision multitier networking and security services from weeks to minutes. Some enterprises use NSX to give application teams full self-service provisioning capabilities. Automation and orchestration capabilities in NSX help you avoid manual configuration errors.

- **Simplifying network traffic flows:** You can use NSX to lessen the load of server-to-server traffic VMs communicate with one another through the vSwitch or aggregation fabric. This cuts down on east–west traffic hops and helps you avoid convoluted traffic patterns and the costs of building up core capacity with more hardware.
- **Enhancing 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.

Economic benefits

The economic benefits of network virtualization with NSX emerge across both capital and operational expenditures:

- **Reducing the risk of costly breaches:** Deploying firewalls and advanced threat protection solutions to control an increasing volume of east–west traffic inside the data center is cost-prohibitive. The sheer number of devices needed and the effort required to manage complex firewall rules have made this approach operationally not feasible. Micro-segmentation and advanced threat protection capabilities that come with network virtualization make this doable and affordable. You reduce the risk of cross-data-center security breaches while avoiding capital expenditures on hardware and software.
- **Reducing time and effort:** Network virtualization greatly reduces the effort and time it takes to complete network tasks. NSX reduces the effort from hours to minutes, and the cycle times from days to minutes. If you consider all the manual tasks — across development, testing, staging, and production environments — and the fact that NSX 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 administrators often overprovision compute to avoid the network reconfiguration required to reach available capacity in another cluster. You can instead use NSX to bridge

network clusters and deploy workloads to the unused capacity. By making better use of existing server capacity, you avoid the need to buy new servers.

- **Improving cost and performance savings:** Many enterprises use NSX and network virtualization to replace expensive proprietary hardware with lower-cost multivendor infrastructure.
- **Extending the hardware life cycle:** You can use NSX to pull more value from your existing network infrastructure. NSX Data Center offloads east–west traffic from the network core, allowing you to extend hardware lifespan. Similarly, protecting east–west traffic in a data center with the NSX distributed firewall greatly reduces the burden on physical firewalls. Instead of refreshing your networking and security gear at the end of the accounting depreciation cycle, you can use it for longer periods. You touch the hardware only to add more capacity or to replace failed devices.

IN THIS CHAPTER

- Reevaluating security
- Understanding multi-cloud networking
- Networking for containers
- Automating across the network stack

Chapter 4
Exploring Network Virtualization Use Cases

Network virtualization improves on the status quo across a number of different use cases. In this chapter, we walk through those categories, giving examples of how people are putting network virtualization into action.

REMEMBER

As we note in Chapter 3, virtualization with NSX 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 with a single use case while establishing a strategic platform that drives additional use cases and projects over time.

In the following sections, we drill down into some common use cases to show how network virtualization speeds up processes, strengthens security, and keeps your applications up and running.

Securing the Data Center

The average cost of a data breach comes with a hefty price tag of around $4 million, so mitigating risk and keeping infrastructure safe are key concerns for chief information security officers (CISOs). Demonstrating and ensuring compliance is equally vital.

Attackers exploit inherent weaknesses in traditional perimeter-centric network security strategies to infiltrate enterprise data centers. After 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 propagation.

There certainly is no lack of security solutions today. According to research, the average enterprise has 75 different security products. Enterprises have purchased a broad set of network and endpoint-based security solutions. Achieving scale and streamlined operations while ensuring compliance is a challenging and expensive endeavor.

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 80 percent of all network traffic.

Attackers have modified their attack strategies to take advantage of this paradigm shift and the fact that perimeter-centric defense strategies offer little control for communications within the data center. Security teams must likewise extend their defense strategies inside the data center instead of focusing exclusively on perimeter defenses.

For the most part, east–west server communications in the data center don't pass through a firewall and are, therefore, not inspected or visible to network security teams. When east–west traffic *is* forced through a firewall — using techniques such as hairpinning — the result is a complex and inefficient communication path that hurts network performance.

Security at the granularity of a workload and the scale of the enterprise

As businesses become digitized, and workplaces expand on remote work and digital customer experiences, securing applications and data across the enterprise is of paramount importance.

Improving the overall security posture includes minimizing risks, deploying consistent security controls, enforcing compliance, and implementing strategies, such as Zero Trust, that maximize protection with granular firewall rules specific to the workload.

Deploying enterprise edge firewalls as internal firewalls

Deploying network security traditionally involves a number of physical firewall appliances at the perimeter or between the network demilitarized zone (DMZ) and internal segments.

Deploying firewalls in a brownfield data center involves significant network re-architecture. Some re-architecture is also required whenever major firewall policy changes are needed. This may involve creating VLANs and routing changes, as well as re-IPing workloads.

All these operations are not only time-intensive but also highly error-prone, which gets amplified in modern data centers that are in constant motion. Applications are continuously being developed, and new applications are being deployed, as existing applications are being virtualized, containerized, moved across the physical infrastructure or data center, or decommissioned.

Modern applications consist of workloads in different form factors residing in different locations. Purchasing the number of firewalls necessary for effective micro-segmentation isn't financially feasible. How many VMs does your data center have? Hundreds? Thousands? This would mean potentially hundreds or thousands of firewalls.

Leveraging a traditional perimeter firewall to secure these workloads is operationally inefficient and leads to unmitigated risk.

Micro-segmentation-only solutions

In 2013, VMware pioneered micro-segmentation. Today, although many micro-segmentation solutions exist, most are purely focused on micro-segmentation and are not suited to replace a firewall appliance. Often these solutions orchestrate an already existing firewall inside each protected workload and lack advanced controls such as stateful layer 7 firewalling, URL filtering, or intrusion detection and prevention.

Internal firewalling with the Service-defined Firewall

Network virtualization provides an ideal layer to insert security, because it's close to, yet isolated from, applications. Network virtualization allows for a new infrastructure architecture with intrinsic security, drastically mitigating the risks of data breaches.

NSX delivers security controls that are intrinsic to the infrastructure. With NSX, you can apply internal firewalling to any workload (VM, container, or physical server) regardless of how it is connected. It could be VLAN-backed with a physical default gateway or overlay-backed with NSX providing a network overlay and distributed virtual routing, and the workload may be deployed across on-premises data centers, in the public cloud, or on VMware cloud such as VMware Cloud (VMC) on Amazon Web Services (AWS).

When a workload vMotions between clusters or data centers, both firewall policy and firewall state moves with the workload.

VMware Service-defined Firewall

The VMware Service-defined Firewall is a distributed, scale-out internal firewall that protects all east–west traffic with security that's intrinsic to the infrastructure. It includes a distributed firewall, an intrusion detection system (IDS) and intrusion prevention system (IPS), and deep analytics through NSX Intelligence.

NSX Distributed IDS/IPS is fully integrated into the virtualization infrastructure, which provides several benefits:

- **Distributed, granular enforcement:** The Service-defined Firewall provides distributed and granular enforcement of security policies to deliver protection and control down to the workload level.

- **Scalability and throughput:** Because it's distributed, the Service-defined Firewall is elastic, with the ability to autoscale as workloads spin up or down.
- **Intra-application visibility:** The Service-defined Firewall automatically determines the communication patterns between workloads and microservices, makes security policy recommendations, and verifies confirmance.
- **Declarative application programming interface (API):** Security teams can move at the speed of development to deliver a true public-cloud experience on-premises. The API-driven policy model ensures that new workloads automatically inherit relevant security policies
- **Centralized management:** Security policies are defined centrally and distributed throughout the network, with the Service-defined Firewall automatically adjusting policies whenever a workload is created or decommissioned.

The VMware Service-defined Firewall is distributed, service aware, and operationally simple. With an internal firewall from VMware, CISOs and their teams can mitigate risk, enable compliance, and move at the speed of development.

Distributed Firewall

The NSX Distributed Firewall is a Layer 2 through Layer 7 stateful firewall implemented at the virtual network interface card (vNIC) of every workload. It sits between the vNIC and the logical switch and inspect every single packet going in and out of a workload. The distributed firewall is also isolated from the workloads it's protecting and doesn't require any components to be installed on the workload. Any level of segmentation can be achieved without making any changes to networking and without re-IPing any workloads.

Traditional network security policies use constructs like Internet Protocol (IP) addresses and Transmission Control Protocol (TCP) ports that are more a result of static infrastructure than application context. By bringing security close to the application, network virtualization enables security policies that are based on the context of the application. This is inherently more secure and easier to manage.

Here are some examples of application context that you might 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, an authentication utility, or a web app? The behavior of the application is best identified at layer 7, past the layer 4 port, which can only take a best guess.
- **Third parties:** What do third-party systems say about this application, beyond the context that the virtualization platform, cloud platform, or hypervisor already knows?

If you apply security tags to workloads when deploying an application, the workloads become a member of a dynamic security group. The appropriate policies are applied to isolate the application. When the workload is decommissioned, policies are automatically removed. In essence, through dynamic grouping, the life cycle of a Service-defined Firewall policy is directly tied to the life cycle of the workloads or applications it's protecting. That is radically different from traditional firewalls.

NSX supports a broad range of service specifications in each firewall rule. L2 service objects include protocols like IPv6 or ARP and enable administrators to block the use of these Layer 2 protocols. The same can be done for Layer 3 protocols like Generic Routing Encapsulation (GRE). Most firewall rules leverage Layer 4 objects, which are a combination of transport layer protocol and port. As an example, the NTP L4 Service Object matches UDP traffic destined to port 123. Beyond these static services, NSX supports application-level gateways (ALGs) and layer 7 context profiles.

Layer 7 objects are port-independent and instead use signatures to match content in the payload of a flow. This enables a firewall to distinguish, for instance, HTTP from MySQL traffic, even if both services run on port 80.

NSX comes with layer 7 context profiles, which map with the services customers commonly run. These profiles can be used on the distributed firewall (DFW) and the tier 1 gateway firewall (GFW). Layer 7 context profiles can be used in combination with a static L4 port-based service object, in combination with an ALG dynamic port-based service object or by itself. Just a handful of packets are required for the NSX firewalls to fingerprint the Application ID (AppID) a flow is generated to or from, which means there is no throughput penalty.

NSX can distinguish among different versions of SSL/TLS. This allows security teams to see and enforce the use of specific protocol versions throughout the organization, even when application owners inadvertently spin up a server accepting client-initiated downgrades to noncompliant versions of the protocol.

Workloads that need to meet compliance can be tagged, and a specific set of rules required for compliance can be applied to only those workloads. NSX also enables administrators to enforce the use of secure cipher suites with TLS. This further reduces the potential for attack by blocking the use of certain vulnerable legacy algorithms that are supported in TLS 1.0–1.2.

Distributed intrusion detection and prevention

In order to detect and prevent attempts at exploiting vulnerabilities in operating systems, applications, processes, and protocols, organizations deploy intrusion detection system (IDS) and intrusion prevention system (IPS) at the perimeter of the network, as well as between data center segments. One key challenge is that it requires a massive amount of traffic hairpinning or copying to centralized appliances. This process often involves network architecture, and you have to continuously keep adding firewalls or IDS appliances to keep up with the growing amount of traffic that needs inspection.

Another challenge with this approach is that it doesn't offer protection against lateral movement of attacks within a particular network segment. When two application workloads are deployed in the same VLAN, there isn't any feasible way to insert an in-line IPS appliance in between these workloads.

Furthermore, workloads often move to other hosts, clusters, or data centers by leveraging Distributed Resource Scheduler (DRS) and vMotion, and traffic redirects to an IPS appliance has no context for the existing flow.

Finally, centralized network-based IDS/IPS have little understanding of flow context. They don't know much about where the flow originated and whether the target is potentially vulnerable. All traffic needs to be matched against several thousand signatures. Signatures that detect an exploit against an Apache vulnerability are also applied to a MySQL server, and so on. This results in a large number of false positives, making it difficult for a security operator to distinguish important events that require immediate action from all the other ones, especially if the events don't include context about who the victim is and what's running on that victim machine.

With the NSX Distributed IDS/IPS, you can deploy advanced threat protection at every workload. This distributed implementation eliminates blind spots and fundamentally changes the trade-offs between coverage, complexity, and accuracy that traditional network IDS/IPS suffer from.

The NSX Distributed IDS/IPS is fully integrated into the virtualization infrastructure, which provides several benefits:

- **No single inspection bottleneck:** The NSX Distributed IDS/IPS uses stranded compute capacity on existing servers. Unlike traditional appliances, it scales out with your workloads with no single capacity bottleneck.
- **Optimized traffic flow:** Typically, traffic flows requiring IDS/IPS inspection are forced to traverse a centralized appliance, creating a hairpin and chewing up network resources. Deploying traditional IDS/IPS appliances involves network re-architecture. NSX eliminates hairpins and optimizes network traffic by co-locating IDS/IPS inspection with the source/destination of the traffic flow.
- **Inspection for all traffic:** Traditional firewalls and in-line IDS/IPS appliances are limited in how much traffic they can inspect and require network re-architecture to force packets through them. You can't apply in-line IDS/IPS to traffic between workloads on the same network segment

or VLAN. With NSX, you can insert IDS/IPS inspection in the path of every traffic flow for every workload.

- **Curated signature distribution and context-based threat detection:** Traditional IDS/IPS appliances have little contextual understanding and typically match all traffic against all signatures, regardless of relevancy. This lack of context makes it hard for security teams to filter noise from critical events that warrant immediate action. This broad application of signatures also impacts performance. The NSX Distributed IDS/IPS has rich context on each guest through VMware tools and Guest Introspection, allowing it to selectively enable only relevant signatures for each workload context, enabling a quicker response and the ability to selectively enable only relevant signatures.
- **Workload mobility support:** With a traditional IDS/IPS, there is no straightforward way to reconfigure security policies for a workload that moves (due to VMotion). With NSX, security policies and state move with the workload and no traffic is dropped.
- **Automated policy life-cycle management:** Traditional IDS/IPS is not aware of application life cycle and need to be modified when a workload is created or decommissioned. NSX uses dynamic group-based tags to directly tie security policies to the application life cycle. When a workload is deployed, the appropriate firewall and IDS/IPS policy is automatically applied. When an application is decommissioned, groups and rules are adjusted. There is no manual process involved that significantly reduces the reconfiguration burden, as well as the associated risks.

NSX Distributed IDS/IPS enables network and security operators to simplify network architecture and operations while utilizing unused server capacity. Because the Service-defined Firewall and NSX Distributed IDS/IPS are applied to every workload, they provide deep security at the granularity of a workload and the scale of the software-defined data center (SDDC).

NSX Intelligence

Traditional security analytics products provide insight at the cost of operational complexity and overhead. They rely on agents or sensors deployed on each workload or on network taps to gather the necessary data for security and network analysis. They duplicate and transmit all this data to discrete, centralized appliances,

each of which performs expensive packet analysis to reconstruct state and layer 7 context. This architectural model places a heavy burden on your network, is expensive, and requires a lot of management overhead on operations teams.

The virtual network layer is uniquely positioned to see all traffic in the data center, down to individual workloads (such as VMs and containers). This level of visibility and context enables segmentation based on attributes unique to each workload, such as the operating system, patch level, running services, and so on. This, in turn, enables more intelligent network and security policy decisions that are defined with the workload context in mind.

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

VMware NSX Intelligence is a distributed analytics engine built natively within NSX. It delivers a more granular security posture, simplifies compliance analysis, and enables proactive security.

By distributing analysis to each hypervisor, NSX Intelligence eliminates the need for large, complex, centralized appliances that most security analytics products require. NSX Intelligence only sends relevant metadata to a lightweight central repository for building machine learning models and further analysis. It doesn't require agents or network taps and processes packets in-line as they traverse the hypervisor. This single-pass approach enables computationally efficient analytics processing, enabling intelligent policy formulation, and network and security analytics.

Key capabilities of NSX Intelligence include

- **Contextual application topology maps:** NSX Intelligence inventories all endpoints and traffic flows, and consolidates metadata and configuration data from NSX, vSphere, and more to provide complete workload context. Workloads automatically get clustered into granular groups in a hierarchical application map that scales to tens of thousands of endpoints and enables drilling down from high-level applications to detailed workload context.

- **Micro-segmentation and firewall policy recommendation:** NSX Intelligence automatically generates rules to micro-segment applications and, with the click of a button, provisions them in the NSX Distributed Firewall. Topology visualization enables iterative micro-segmentation planning.
- **Stateful layer 7 processing:** The NSX distributed firewall engine processes every packet with complete state and layer 7 context, including protocol and application ID.
- **Comprehensive packet inspection:** NSX Intelligence continually monitors every packet between every workload without any sampling to enable context-based flow visualization and rapid security analysis.
- **Efficient and distributed in-line processing:** Packet processing and workload analysis are distributed to each hypervisor. The processing is done in-line with the distributed firewall within the hypervisor, making it highly efficient with minimal overhead.

Taking a phased approach to securing a data center

Most organizations follow an iterative approach to improving their data center security with an internal distributed firewall.

Many VMware customers use an approach consisting of four distinct phases. You can achieve any of these levels of segmentation without changing the underlying network or re-IPing workloads.

Crawl: Macro-segmenting the network

In this phase, the network is segmented using virtual security zones. Depending on business needs and use cases, you could begin by segmenting environments that should not directly communicate with each other. Examples include different business units, partner environments, and development and production environments. This immediately prevents attackers from moving between environments.

Walk: Protecting critical applications

The next phase is to enforce more granular controls down to the workload level. In this phase, organizations choose one or more well-understood applications that are critical to the business and

that should be protected with additional security controls to prevent unauthorized access, data breaches, and other attacks. You can further enhance this by enabling built-in IDS/IPS.

Jog: Gaining visibility and securing additional applications

As your security team gains more experience in operating a distributed internal firewall, you can continue expanding your monitoring and protection of east–west traffic. In this phase, you use the built-in visibility and automation in the Service-defined Firewall to isolate and secure more applications.

For applications that are less well understood, NSX Intelligence provides data-center-wide visibility and machine learning techniques to help you understand applications and traffic flows. Automated application discovery provides a comprehensive map of application topography, along with security policy recommendations based on observed traffic flows.

Run: Securing all applications

Now your team has achieved organizational maturity with internal firewalling. You have the skills and experience to secure the remaining applications. Network and security teams can now move at the speed of development. With its API-driven, object-based policy model, the Service-defined Firewall helps accelerate security operations. This ensures that new workloads inherit relevant security policies with automated policy mobility.


TIP

If you haven't already deployed advanced threat detection and prevention using IDS/IPS for your sensitive applications, now is the time to do so. This will help you achieve regulatory compliance for the Health Insurance Portability and Accountability Act (HIPAA), PCI DSS, and other mandates.

Securing user environments: Micro-segmentation for VDI

The COVID-19 pandemic has forced many organizations to shift their businesses online and require employees to work from home. Businesses have had to quickly adjust and scale up their infrastructures, sometimes with security as an afterthought. Malicious actors immediately began taking advantage of this new reality by

targeting vulnerabilities commonly associated with employees accessing corporate resources from their home environments.

VMware solutions ensure business continuity so employees can work from home with secure and reliable access to corporate resources and applications. Virtual Desktop Infrastructure (VDI) reduces the impact on productivity and risk associated with accessing internal data and applications remotely.

Protecting desktop pools

With VDI, user desktops reside within the data center, close to the severs hosting critical applications and data. Humans are the weakest link in a security chain, so bringing them within the data center through desktop virtualization can present a new threat vector. Isolating VDI pools and Remote Desktop Session Host (RDSH) farms from the rest of the data center is crucial. Providing this segmentation at scale, without requiring network re-architecture, is key.

The VMware Service-defined Firewall groups desktops using dynamic security groups based on criteria such as VM name, network segment, or security tag. Appropriate segmentation policy is applied, isolating them in the data center. New desktops can be quickly added to existing groups for massive scale-ups. The same segmentation policy is applied as soon as a new desktop comes up, without any policy changes, changes to the network, or adding new physical firewall appliances.

In the traditional model, traffic to or from desktop pools is hairpinned to a physical firewall. Because they're based on IP subnets, firewall policies don't scale and need to be manually adjusted for large VDI pools. This is error-prone and often slows down the rollout.

Similar to how attackers move laterally within an environment, ransomware and other malware often exhibit wormlike behavior, spreading from one infected machine to another. You may be familiar with the WannaCry ransomware attack, which exploited the EternalBlue vulnerability in Windows SMBv1 servers. WannaCry is executed on one machine and scans the rest of the environment to propagate laterally.

WARNING

Microsoft recently published a security advisory on a remote code execution vulnerability impacting SMBv3.1.1 clients and servers on Windows 10 and Windows Server operating systems. This vulnerability, commonly referred to as SMBGhost or CoronaBlue, is similar to EternalBlue in that it is considered wormable, meaning it can self-propagate over the network.

Although network-based segmentation can help prevent lateral movement between zones, it doesn't offer protection against propagation within a subnet such as a desktop pool. The NSX Distributed Firewall, on the other hand, literally sits at the vNIC of every workload and has the ability to intercept traffic before it hits the network, regardless of whether that traffic is going to the Internet, a production application, or another desktop.

The beauty of this architecture is its simplicity. With just a single rule on the NSX Distributed Firewall, you can isolate every single desktop. Using dynamic security groups based on tags or other constructs, policy is automatically applied to every desktop that is spun up. With a single desktop isolation rule, NSX customers can stop the self-propagation of ransomware across their desktops, as well as the lateral movement of an attack.

For lateral communication between desktops, you can enforce more secure protocols using a layer 7 firewall policy that uses application identity. Additionally, NSX uses distributed IDS/IPS to detect exploits, whether it's an attacker attempting to gain a foothold or ransomware spreading from desktop to desktop across an allowed port on the same network segment.

Enabling user-based access control

Most organizations have distinct desktop pools for contractors and employees with policies that only allow employees to access internal applications. But often, a more granular policy application is required. For instance, within the "employee" pool, the medical staff should be able to access their medical records application but not HR applications, while the opposite is true for HR users, regardless of which VDI desktop or Remote Desktop Session (RDS) host the user has.

A Service-defined Firewall enables user-based firewalling, commonly known as *identity firewalling* (IDFW). With IDFW, you can create firewall rules based on Active Directory user groups to

provide granular per-user access to applications. NSX Identity Firewalling can be applied to both users accessing apps from individual VDI desktops and multiple users accessing published desktops or applications through an RDS host. With NSX-T, IDFW-based rules can also use layer 7 and/or FQDN context profiles for more granular per-user control.

Protecting VDI infrastructure

Virtual desktop solutions consist of many different workloads, such as Unified Access Gateways and connection servers that need to interact with other infrastructure components, such as Active Directory servers, DNS, or VMware vCenter. Ensuring proper controls for access between the outside world and the VDI components is critical for ensuring a secure infrastructure upon which secure desktops can be delivered.

Many customers use NSX to microsegment their Horizon deployments, leveraging security that scales with the applications. By using dynamic security groups in the VDI micro-segmentation policy, policy application becomes automatic. When infrastructure components like connection servers need to be expanded, appropriate policies are automatically applied to new servers without requiring policy reconfiguration.

Multi-Cloud Networking

According to the *Flexera 2020 State of the Cloud Report,* enterprises have almost entirely embraced multi-cloud. Ninety-three percent of respondents reported having a multi-cloud strategy. Organizations that avoid public clouds due to regulatory issues still manage multiple private data center clouds (private clouds) to improve application continuity. Organizations that do use public clouds may have one developer spinning up an app in AWS while another is doing so in Google Cloud Platform. Meanwhile, a whole separate team may have a complete project in Azure.

Managing IT processes, planning for disasters, and 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 by removing several barriers.

Managing hybrid cloud environments

Multi-cloud architectures are complex and need multi-cloud tooling to manage cloud resources cost-effectively and ensure strong security. However, when the network is virtualized, extending its benefits to the cloud becomes a simple add-on.

VMware NSX Cloud does exactly this by adding cloud-native workloads to NSX Data Center, while using a common management portal. NSX Cloud includes many of the same features such as distributed firewall, service insertion, IPsec VPN, Layer 3 Switched Port Analyzer (L3SPAN), and IP Flow Information Export (IPFIX). Both share the same management and control plane with centralized policy management and control.

VMware Cloud, available on all major cloud platforms including AWS, GCP, and Azure, offers consistent infrastructure and operations for those using VMware technologies on-premises. With the same VMware SDDC stack of vSphere, vSAN, and NSX across on-premises and cloud, enterprises enjoy a consistent environment to reuse skills, scripts, APIs, and operational tools.

Disaster recovery and metro pooling

NSX Federation simplifies disaster recovery (DR). It's orchestrated and integrated across compute, storage, networking, and security. NSX is also compatible with DR orchestration tools, such as VMware SRM, Dell EMC RP4VM, Zerto, and Veeam.

NSX 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 policy spanning 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 networks for test recovery plans without disrupting production. Testing is isolated and maintains the same application IP addresses and policies at the recovery site.

Multi-site pooling creates a unified, seamless, and resilient pool of infrastructure to run applications across multiple data centers and to the cloud. Applications can be deployed in any location and can connect to resources across sites for disaster avoidance, planned and unplanned outages, or better resource utilization.

Consistent security policy and visibility

NSX Data Center and NSX Cloud together provide a unified networking and security model that delivers high-fidelity security policy throughout the network. Security mechanisms such as micro-segmentation and IDS/IPS are applied to traffic between workloads in the cloud or in the data center.

You can define a security policy from a centralized NSX Global Manager and apply it to workloads anywhere — across cloud virtual networks, regions, availability zones, and multiple private data centers and public clouds. Security rules follow workloads when they're moved. Network and security policies are dynamic and easy to configure. This is extremely useful in a multi-site environment where workloads and networks need portability. You can define policies based on rich constructs such as workload attributes and user tags and respond to threats gracefully with a quarantine of rogue or compromised cloud endpoints.

Workload mobility between clouds

Enterprises are increasingly using advanced workload mobility between private and public clouds, allowing them to efficiently plan downtime and scale their network. With Layer 2 VPN (L2VPN), NSX Data Center helps deliver secure and seamless application mobility, making it easy to migrate to and from the cloud or between physical sites.

VMware HCX, available alongside NSX Data Center, is an application mobility platform designed to simplify application migration, workload rebalancing, and business continuity. HCX addresses several major challenges with multi-cloud migration:

- **Migrating applications:** Schedule and migrate thousands of vSphere VMs within and across data centers without requiring a reboot.
- **Changing platforms or upgrading vSphere:** Migrate workloads from vSphere, KVM, and Hyper-V environments within and across data centers or clouds.
- **Workload rebalancing:** Move applications and workloads across cloud regions and cloud providers to achieve scale, cost, compliance, and vendor-neutrality goals.

- **Business continuity and protection:** Protect workloads by replicating them to other HCX-enabled site in a scheduled or on-demand fashion.

Networking Modern Applications

Containers and microservices are emerging as the dominant software development pattern for modernizing applications. Kubernetes, an open-source project governed by the Cloud Native Computing Foundation (CNCF), has become the de facto container orchestration platform. *CNCF Survey 2019* shows that 78 percent of respondents currently use Kubernetes in production up from 58 percent in 2018. Eighteen percent of respondents run more than 5,000 containers in production.

Networking in Kubernetes is accomplished using a Container Network Interface (CNI), a specification for writing plug-ins to configure network interfaces for containers.

NSX Data Center implements a CNI called NSX Container Plugin (NCP), which provides full-stack networking and security for Kubernetes. This prescriptive network design automatically implements the logical segments, routing and firewalling, and IPAM services required for Kubernetes clusters. Administrators can apply security policies at a VM, pod, or container level, and workloads automatically inherit the required policy applied, allowing developers to self-service resources.

NSX takes a modern approach to load balancing, application security, and Kubernetes ingress, providing elastic, reliable, and highly automated application services. Developers can leverage the NSX Advanced Load Balancer to implement Kubernetes ingress for exposing their applications to the external world.

This converged approach to Kubernetes networking allows enterprises to standardize on NSX across VMs, containers, bare-metal servers, or wherever their applications are deployed.

Automating the Network

Manual processes are arcane and a drain on the budget. Network virtualization automates labor-intensive, error-prone network configuration, provisioning, management, and more.

Network automation

Network automation is a means to doing things faster. The decision to automate is usually complex, often driven by business goals and the need for a more reliable, scalable network.

Network automation is the prime way to take advantage of the programmatic interface exposed by modern solutions that offer an API. APIs deliver structured data rather than raw text (for instance, the output of a log) that network engineers can use to streamline day-to-day operations and network management, network analysis, and troubleshooting.

TIP

The network automation capabilities of NSX enable you to

- Automate repetitive tasks and replicating with templates.
- Build a more stable, reliable network.
- Analyze issues and solve them faster.
- Reduce operational expense.
- Speed up service delivery and accelerate time to market.

Developer cloud

Developers, app owners, network administrators, and security engineers all expect a quick turnaround on resource requests. However, limited management tools, lack of governance, and cumbersome processes often create a barrier for quick turnarounds.

VMware NSX is ideally suited for use as a networking and security platform for workloads in self-service developer clouds. Automated network and service provisioning gives your development and test teams fast access to the infrastructure, so they can get apps and upgrades quickly into the hands of users.

NSX can provision thousands of isolated networks for development, testing, and staging — all on the same physical infrastructure. You can use popular configuration management tools like Ansible or Terraform to manage NSX. Ansible NSX modules and NSX Terraform providers are open source and available for free. You can create and save your entire network configuration in a playbook or manifest file and revision-control them, making a true infrastructure-as-code solution.

Networks are deployed in lockstep with workloads. Applications quickly move through development, testing, staging, and production without changes to their IP addresses.

IN THIS CHAPTER

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

Chapter 5
Operationalizing Network Virtualization

To *operationalize* something means to put it to real-world use. Operationalizing network virtualization is the process of optimizing people, processes, and technology to maximize network virtualization 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

On your journey toward network virtualization, you should consider three key operations investment areas — people, processes, and tooling. 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 people, processes, and tooling. We cover each of those areas in detail in the upcoming sections.

People and processes

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 and security staff that they will not be automated out of jobs and that their jobs will not be moved to the virtualization team. Your existing staff takes on network virtualization. Only they have the required networking and security 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 virtual networks are as secure as physical networks. Virtualized security services such as micro-segmentation, intrusion detection system (IDS)/intrusion prevention system (IPS), and other advanced threat protection services do not replace existing perimeter firewalls for north–south traffic; instead, they allow your organization to control east–west traffic inside the data center in an agile, cost-effective manner that further enhances defense in depth.


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 up-front 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 from 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; 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 and 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

You can use network virtualization for a number of things. 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

- IT staff rack and stack physical devices and manually configure them through command-line interfaces (CLIs) or scripts.
- Ticketing systems (for example, ServiceNow) generate multiple requests and track status.
- Network configuration management (NCM), configuration management databases (CMDBs) such as HP Network Automation (HPNA), and compliance tools track configuration items and their relationships.

Ideal state

- Orchestration/cloud management platform (CMP) tools (such as vRealize Automation, Chef, or Puppet) provide automation for provisioning and configuration management.
- Self-service portals provide catalogs of services and automation with APIs.

- Standardized templates include built-in relationships. You can leverage APIs to discover the network 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.
- External monitoring tools provide auto remediation 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 which 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's built-in Flow Monitoring and Endpoint Monitoring tools). Repeat with the next application.

Developing the Right Mindset

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, advanced threat protection, 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 administrators, engineers, and architects to become leaders in a new paradigm of networking and security. This requires a mindset focused on finding opportunities rather than believing your abilities are fixed.

TIP

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 administrators 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.


TIP

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. We provide a library of resources on network virtualization, highlight opportunities to deploy the VMware NSX with Cisco infrastructure, and explain how NSX integrates with existing infrastructure and third-party solutions.

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/Yu9WLtFWiPQ`):** This three-minute video explains how NSX provides full-stack layer 2 to layer 7 network virtualization and security across data

centers, clouds, and applications running on VMs, containers, and bare-metal servers.

- **VMware Service-defined Firewall Introduction Video (**`https://youtu.be/2wigl10t0fE`**):** This short video introduces the VMware Service-defined Firewall, a distributed, scale-out internal firewall purpose-built to protect east–west traffic.
- **The VMware NSX Data Center product page (**`www.vmware.com/go/nsx`**):** The NSX Data Center product page summarizes the features, functions, and benefits of the NSX Data Center platform. It also provides a wide range of deep-dive assets, technical information, and business-focused content.
- **The VMware Service-defined Firewall product page (**`www.vmware.com/security/internal-firewall.html`**):** The VMware Service-defined Firewall product page summarizes the basic features, functions, and benefits of the distributed, scale-out internal firewall built on NSX that secures east–west traffic across multi-cloud environments.
- **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.

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-T Solution Overview (**`www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-solution-brief.pdf`**):** This solution brief describes the Layer 2 to Layer 7 networking

and security services delivered by NSX. It describes the primary NSX use cases, including multi-cloud networking, security, modern applications, and automation.

- **VMware NSX-T Data Center Reference Design Guide (**`https://communities.vmware.com/docs/DOC-37591`**):** This detailed reference design guide for NSX-T doesn't require any familiarity with NSX Data Center.
- **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:
  - *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 the latest news, deep technical insights, and how-to tips about network virtualization.

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

To enrich your understanding of a platform, it always helps to hop into the driver's seat for a test drive. VMware NSX-T Hands-on Lab (`https://my.vmware.com/en/web/vmware/evalcenter?p=nsx-t-hol-dc-20`) delivers a fully operational live desktop environment 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-T Data Center without installing any software.

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`). Get insights within 24 hours. The VNA will

- Show your network traffic distribution by type (east–west, Internet, and by services (web, database, 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.

Deploying NSX in Your Environment

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

Start your journey by learning about the fundamentals of network virtualization and the business challenges NSX Data Center can help solve. You can take a self-paced, on-demand course on how

to install, configure, and manage NSX Data Center. To learn more, check out the following:


TIP

- **Coursera (free; `http://vmware.com/go/coursera`):** "Networking and Security Architecture with VMware NSX" on Coursera provides information on basic networking virtualization with VMware NSX.

  To get the most out 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?ui=www_edu&a=one&id_subject=74570`):** A three-hour self-paced online course that will provides 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 environment with the following courses:
  - **VMware NSX: Install, Configure, Manage:** A five-day course on how to use logical switching and routing, gateway services, firewall, 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 to bridge the physical and virtual worlds using the level 2 gateway. 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 partners to create reference architectures and design guides for using NSX Data Center as an agile overlay.

Here's a sampling of the technical resources available:

- **Arista:** VMware and Arista Network Virtualization Reference Design Guide for VMware vSphere Environments (`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

NSX Data Center is designed to integrate with solutions for various network services:

- **Physical-to-virtual data center services:** Arista Networks, Dell EMC, 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, secured, 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®

Varun Santosh has worked more than 10 years in networking and security, designing and building data center, WAN, and cloud networking products. He received his BE from University of Mumbai and his MBA from UC Berkeley Haas. **Stijn Vanveerdeghem** is a Senior Technical Product Manager with more than 10 years of experience in security. He holds a bachelor's degree from the Catholic University College Sint-Lieven and a CCIE in Security. He is a regular speaker at events including VMworld, Palo Alto Ignite, and Cisco Live.

ISBN: 978-1-119-73684-4
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.