Planning for operational transformation with NSX

Real world best practices

GUIDEBOOK

vmware®

Table of Contents

Introduction

This white paper is primarily for cloud, networking, and security executives and managers. It is also helpful for managers and individual contributors in architecture, engineering, and operations who are participating in operationalizing NSX at their organization.

Network virtualization represents a major advancement in helping organizations realize the benefits of speed, agility, and security. It is equivalent to or greater than the benefits that compute virtualization provided over the past decade. To realize the benefits of network virtualization, organizations will want to assess and execute an operational plan that spans across **people**, **process**, and **technology**.

VMware worked closely with existing NSX customers to understand the realities of putting network virtualization into production. This real-world knowledge will help guide you through the evaluation, deployment, and operationalization of NSX. You and your organization can review and make use of the best practices that make the most sense for your particular situation.

While this paper covers a broad spectrum of best practices, NSX can be operationalized with minimal changes to start, regardless of your current state. Operationalizing NSX is not complicated, and there's a clear path for success.

This guide is divided into three main sections that address key learnings and best practices for:

People

Network virtualization offers the potential to unlock organizational strengths and major benefits of transforming how work gets done across the technology organization. It also represents a change that needs to be carefully considered to ensure clarity and alignment across the organization. Ensuring you have an agile organizational structure, with blended teams that have clear roles and responsibilities, will allow you to derive the greatest outcomes and value for your organization and staff. We provide information and guidance on organizational structures, internal engagement and communication strategies, and roles and responsibilities.

Process

Network virtualization provides tremendous opportunities to increase productivity through the automation of manual processes across the application life cycle. Defining an ideal future state for how you provision, manage, and monitor applications and services will allow you to move away from unnecessary existing processes and practices. We will give you guidance on how to think about automation, process management, tooling, and some interesting use cases.

Technology

One of the main advantages of network virtualization is the decoupling of network and security functions from the underlying physical network infrastructure and abstracting them into a virtualization layer. This allows you to better architect and manage your infrastructure moving forward. We will provide guidance on architectural best practices, incremental implementation of infrastructure, and periodic rollout of new capabilities.

These best practices are not meant to be prescriptive or "one size fits all." You need to choose those you believe will work for your organization given its unique characteristics, goals, and priorities. Do not attempt a Big Bang approach. Start small with a couple or a few, then address others over time.

Some organizations get complacent and stop short on their journey to optimal performance. As a result, they limit the success that can be achieved for their organization. Always keep the end state in mind, and continually strive to improve and reach it.

People

The first topic we want to address is people: the organization, teams, and individuals who comprise your technology organization responsible for the end-to-end delivery and management of apps and services and, ultimately, the driving force behind the successful operationalization of network virtualization and security.

Initial thoughts on organizational structure

Network virtualization and NSX do not require a particular type of organizational structure. The optimal structure depends on factors that are unique to your organization. NSX has been operationalized in traditionally siloed organizations to fully blended and embedded cloud teams. Midpoints also exist between strictly siloed and fully blended teams.

Your ideal organizational structure will depend on numerous factors. The following should be taken into consideration when designing the structure:

- Alignment among domains and disciplines
- Maturity of the value stream
- Level of technical leadership
- Experience and expertise of staff
- Operational experience and sophistication
- Use of outsourcing
- Quantity of infrastructure and applications
- Brownfield or greenfield deployment

Our recommendation: design a blended team structure

Based on real-world experience, the most productive teams are tightly woven, highly collaborative, and self-sufficient. These blended teams are proven to work more efficiently, with shorter cycle times, with condensed and amplified feedback loops, and with more knowledge sharing and continuous learning. Ideally the team is co-located.

We have seen successful organizational structures made up of teams based on domain (e.g., compute, storage, networking, and security), and based on discipline (e.g., architecture, development and integration, operations, and support). In both cases, the teams are responsible for physical and virtual infrastructure.

As you move more infrastructure and applications from your existing corporate network to your cloud, the allocation of people will also shift. Over time, more staff members will be working on the cloud and fewer working on the existing corporate network. It is important to develop a communication and training plan to help the organization understand and be prepared for this evolution as well as new career opportunities. Equally as important, you will want to communicate the fact that, regardless of whether an individual is working on the existing corporate network or the cloud, that individual's contribution is essential to the overall success of the organization.

Align with shared measures of success

An important next organizational consideration is alignment with a shared strategy that has well-defined goals, objectives, measures, and incentives. Your team should have a service-oriented approach and be collectively responsible for the entire service delivery life cycle, from business requirements to operating and managing a high-quality production workload that is backed by an SLA.

Each team should also have shared measures of success based on factors that matter most for your organization. Examples include: time to market, impact on revenue, market responsiveness, rate of innovation, and/or customer benefits and satisfaction. The goals should be outwardly focused on the business and consumers of the service.

Allow the team to develop and track its own measures of success. But ensure that measures are relevant and aligned to the shared goals and objectives. In addition to aligning to organizational goals, the key performance indicators should be specific, clear, quantifiable, and measurable. Whatever key performance indicators the team chooses, they should keep it simple and start with a few basic metrics that are easy to understand and meaningful.

After you have chosen your key performance indicators, baseline and document where you stand today. Periodically track and assess your progress (e.g., typically monthly or quarterly) in moving towards the desired end state. Make it clear to the team that they are doing this not to criticize people or past performance, but to show proof of the team's success and the new value they are delivering to the business. These measures can also be used to make performance review and evaluation more effective, tangible, and meaningful for the individual.

Creating an accountable and engaged culture

Culture is an important underpinning of success with network virtualization and security. Having a culture that is supportive of the principles of a software-defined data center is crucial. Rather than mandate cultural change from the executive or management level, which is fundamentally very difficult, culture should emerge organically from within the teams through their shared experience, skills, and values.

By establishing shared measures of success, a new culture will emerge and take root naturally. The foundation of the new culture will be based on a clear business and consumer-focused goal, shared responsibilities and risks, closer collaboration and cooperation, and mutual trust and respect.

The team: security and networking expertise working together

One of the main advantages of network virtualization is the decoupling of network and security functions from the underlying physical network infrastructure and abstracting them into a virtualization layer. This shift has created some questions, such as: "Which team is responsible for virtual networking and security running in the hypervisor?" and "How does network virtualization change my responsibilities?" In this section we answer these questions.

Your existing network and security staff take on network virtualization and security. NSX is based on networking concepts and technologies that require networking expertise. Only your network teams have the required expertise. Network and security experts are needed to design, deploy, and operate virtual networks, just like they are with physical networks.

The physical network does not go away—but it does become much simpler and easier to manage. We do not recommend creating an arbitrary team boundary along the physical and logical networks. To help maximize speed and agility, one team that includes network architects, engineers, and operators should be responsible for the physical underlay and virtual overlay.

You may still choose, however, to have network engineers who focus more on racking, stacking, and configuring the physical equipment, and others who focus more on the virtual overlay. But, all of these people should be a part of the same team.

The networking disciplinary functions (e.g., architects, engineers, and operators) evolve to include network virtualization and security. Most people in networking and security will need to learn something new to enhance their expertise and skills. With NSX, network services are running in the hypervisor layer. Network professionals must have some understanding of server virtualization and what it means to logical network services.

People best practice: training

Early in the evaluation process, the highest priority is to make sure everyone understands the principles of network virtualization and is trained on NSX and related operations and management tools that are part of the cloud ecosystem. VMware offers a number of ways to do this, including hands-on labs, workshops, and courses. These resources are primarily for network professionals who don't have a server virtualization background, but they are suitable for server virtualization professionals who are trying to learn about network virtualization. You can also implement a program to ensure intra-team and inter-team knowledge sharing and training by providing leadership opportunities for individuals to informally teach best practices to other teams and groups.

One of the best ways to accelerate learning is to identify and start a small pilot project and evaluation. Involve all of the necessary disciplinary functions—architecture, engineering, and operators—across compute, storage, networking, and security.

Start with a small, cross-functional team

Another low-risk recommendation is that you start with a small, cross-functional team in your progression toward network virtualization. If you are able to move from siloed to blended teams, do so in stages, over time. We've seen mostly two types of cross-functional teams. Choose the model that works best for you:

Incubation team	Tiger team
If you are able to move to a blended team in the long run, use an incubation team. The incubation team will eventually become a permanent part of the organizational structure/chart. And, have full-time employees who spend 100% of their time with the team.	If you are not able to move to a blended team in the long run, use a tiger team. The tiger team bands and disbands, as needed. Members work on the team part-time and formally report to a different team. We've seen tiger teams used mostly in governmental organizations.

The cross-functional team typically has end-to-end responsibility for a specific application stack or set of application stacks. The team should have experts from compute, storage, networking, and security. Disciplinary skills should span architecture, engineering, and operations. The team must be able to handle everything, from design, development, and testing to deployment and ongoing operations. (Refer to the Appendix for descriptions of the networking and security roles and responsibilities.)

Selecting the change agents for the first team

Choose people for the initial team who are change agents, subject matter experts, evangelists, and respected leaders. Find the people who everyone wants on their team. People who know how to build interpersonal relationships, open communication paths, and identify and minimize points of friction. The champions who encourage others to make the change and lead by example. If the team is not co-located, bring them together at the beginning of the project for a couple of weeks.

Members of the team should have personal MBOs that are aligned to the goals of the team. As an example, if a team member spends 50% of their time on the incubation team, then that work should represent approximately 50% of their MBOs. This may seem obvious, but we have seen cases where the time someone spends with a cross-functional team is treated more as a hobby rather than a core part of their job. This is likely not a path to success.

People best practice: avoid surprises

Don't surprise anyone just before you want to deploy. There have been cases where people in network or security operations were involved too late in the process. As a result, projects were significantly delayed. Operations will need to know how network virtualization and security changes monitoring, alerting, and troubleshooting. And, how their processes and tooling must evolve, which we discuss later in this paper.

Celebrating success and growth opportunities

When engaging networking and security on the project, explain the potential personal and professional. As you virtualize and automate the infrastructure, your networking and security staff will gain more time to work on new and interesting projects. They can focus on strategic initiatives that deliver higher value to the business. For example, rather than the mundane work of configuring VLANs, load balancers, or firewall rules, they can work on designing new services that add value for the business: automating cross-domain processes, designing for resiliency, capacity planning, or other interesting projects and initiatives.

Also explain that the organization's innovators and forward thinkers have an opportunity to contribute to the networking and security transformation. The outcome will be beneficial to those who drive the transformation, just like it was for those who championed and built their careers on IP networks and, more recently, compute virtualization. In both cases, new breeds of administrators were born with new skills and knowledge. Participating in the transformation will enrich people professionally and increase their opportunities and value in the job market.

Promote active engagement with users of the service

Another positive way to promote the team is to engage with consumers of the service (e.g., application, business, and infrastructure owners) to educate them about the new capabilities. Ask for their active participation, and get their requirements and feedback. They will want to know how the capabilities and user experience will change. Several successful engagement activities include:

Regular touch points: conduct periodic workshops to provide updates, capture requirements, and solicit feedback.

"Show not tell": establish and communicate that the team has a regular cadence for developing and releasing new capabilities, which will increase customer engagement.

Communicating success across the org is a good thing

In addition to promoting the project to the chosen team members and consumers of the service, it is also wise to evangelize the project across the lines of business or the entire organization. The goal is to build a critical mass of people who support the project, and to establish the platform as the de-facto way of doing things. Share interesting stories about the business and IT outcomes of the project. You can do this

promotion through a combination of presentations, talks, articles, blog posts, social media, email, or demonstrations. Everyone on the team should think of themselves as an evangelist of the project. Celebrating success, both small and large, is the hallmark of high-performing organizations and should be considered an important best practice in technological change management.

Change is hard: finding shared understanding

We all know that change is hard. Especially in areas and disciplines where change is slow, or in places where change may be perceived as potential threats to a career or livelihood. These factors may create resistance to progress. Some people may actively work against the transformation. The best approach is to seek shared understanding of the potential of network virtualization through authentic communication and advocacy as well as the championing of the organization's successes. You need to be transparent, open, and willing to articulate and answer "What's in it for me? What's in it for us?"

Process

In this section we will explain the impact network virtualization has on operational processes, describe the steps you should take to dissect and understand your existing processes, and make recommendations on how to evolve your processes and tools to take full advantage of network virtualization and security.

Inventory and analyze existing processes

A key value proposition of network virtualization is the automation of typically manual processes associated with the application life cycle. This provides you with a great opportunity to do a holistic assessment of your existing processes to determine how they move forward with network virtualization.

An important tip: do not simply retain all existing processes with NSX network virtualization and security. Doing so will degrade the benefits and cost savings you would otherwise achieve. Identify and understand all of your existing network and security processes. Understand the impact network virtualization has on the following processes:

- Application provisioning
- Configuration management
- Change management
- Capacity management
- Incident and problem management

You will want to understand how these processes work today, from end to end, and how they can be simplified and streamlined via automation and orchestration. You will find that existing processes or steps can be significantly streamlined, or even deprecated in some cases.

After you have taken a thorough inventory, determine your priorities for automating these network and security processes. For quick wins, focus on addressing areas that are of high value and low effort. Do not try to streamline too many processes at one time; choose one or two to get started.

Process best practice: benchmarking

It's important to benchmark before getting started. Before you change anything, baseline and document how long your processes take today. Calculate task effort and cycle times associated with each process. Take these same measurements after you have automated the process. Now you can compare and communicate the results you've achieved. Understanding performance will help the team achieve its objectives (e.g., reducing provisioning time or time to detect and isolate issues), and help them establish proper SLAs for your users.

Automate provisioning and management

Once you have inventoried and assessed your current processes, the next step is to look to automate provisioning and management of your applications or services. Organizations use the inherent automation capabilities of network virtualization and NSX to achieve speed, standardization, consistency, and auditability. Automation also reduces downtime and security risks associated with manual configuration errors. Automation improves development and testing productivity, speeds time to market for new applications, delivers standardized and consistent configurations, and results in fewer errors and faster resolutions.

While NSX does not require automation tools, most customers use a combination of tools and NSX APIs for cloud automation. These tools and APIs are used to automate provisioning and management of NSX functional services for virtual networks (i.e., logical L2 switching, L3 routing, load balancing, firewalling, and edge services). Most organizations using NSX automate multiple services.

Today's typical situation: physical networks and VLANs are still provisioned manually today, on specialized hardware, with keyboards and CLIs. As a result, network changes are in the critical path for application deployments. As you know, these deployments can drag on for days, weeks, or longer—until the network connectivity, performance, availability, and security are ready.

Moving forward with NSX: organizations use NSX to automate the provisioning, configuration, management, and decommissioning of network virtualization and security. With NSX, network teams do not need to configure the multitude of physical switches with traffic steering and network configurations, such as VLANs, VRF, VDC, QoS, ACL, etc.

Once the initial configuration of the physical network is done as an underlay network, the ongoing and frequent reconfiguration with new application deployments or changing application requirements is no longer required. All of those changes now happen in the logical network space using automation tools.

Process best practice: focus on IT automation

We recommend that you begin by building automation for IT, allowing them to fulfill service requests faster. After IT has been automated, you can add a self-service portal and service catalog for application developers and QA engineers to access complete environments with the click of a button. Let's now look at some of the automation tools used by NSX customers.

Tooling considerations

As discussed earlier, it is important that you first identify, understand, and document the tasks and processes you want to automate. This is a key step because IT automation tools, such as cloud management platforms and orchestrators, offer different features and functionality. All of these tools require some upfront investment to learn and setup, and the benefits are worth it.

Look at vRealize Suite and OpenStack for provisioning, management, and orchestration of your network infrastructure. Start by automating discrete tasks to get familiar with the tool. After you have learned the tool, you can move to workflows where the application and its networking and security are provisioned and managed together in a full stack. The network operator or the cloud network operator should be involved in the evaluation and operation of any tools that drive network automation.

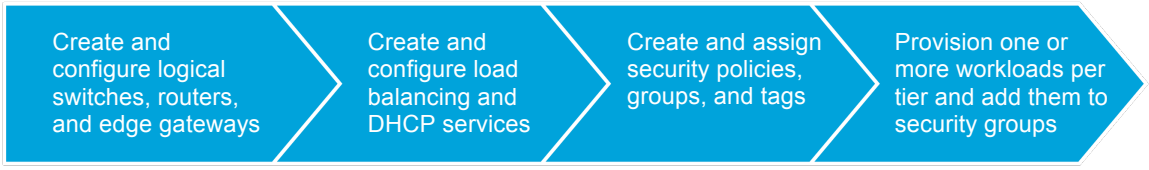
Standardization and customization of configurations

Organizations can standardize the compute, storage, network, and security configurations of full application stacks using templates and policies. If they need to make a change, they modify the template and push it to production. All of the workloads using it will have the change reflected automatically. A record of all changes is maintained for audit and compliance.

Engineering can publish static and/or customizable configurations. Static environments are typically used for production-certified stacks. And, customizable environments are for development and test sandboxes. Customizable environments may address 80% or more of the user's requirements, but can be changed by the developer or QA engineer, as needed. Workloads can be spun up with new networks or to connect to existing networks.

Blueprint process automation example

Let's take a look at the tasks that can be automated for a standardized, three-tier application blueprint:



After the blueprint is tested and validated, it is published to the service catalogue for users to consume. The user clicks on the service item and the entire application stack—with all of its connectivity, availability, and security—is deployed in seconds.

This automated service is many times faster than a traditional physical network without NSX, which typically takes days or weeks. Organizations avoid the long cycle times and delays from complex ticketing workflows, change reviews and approvals, redundant requirements discovery and validation, and manual configuration.

Process best practice: role-based access

Implement role-based access control to the self-service portal based on business roles. You should also define resource reservation and allocation policies according to business groups, track costs for charge backs, and commit to service levels (SLAs).

Automate security policies with groups

NSX natively automates many tasks that are done manually with physical network and security infrastructure. For example, it offers new ways of defining and applying security policy to VMs in the virtualization layer.

Old approach: in the old way, security teams manually create rules based on IP addresses, ports, and protocols. The dreaded "5-Tuple" management nightmare.

New approach: in the new way, security policy is based on security groups. You can define a security group that consists of a set of VMs and create a security policy around those workloads. If you add another VM to the group, the security policy is automatically applied to the new workloads without any manual intervention. Group membership can be dynamically applied via security tags and context as well/instead. NSX security policies may include firewalling, antivirus, and IPS, for example.

Security groups can be static or dynamic—programmed to trigger on just about any arbitrary metadata about the workload. For example, user group identity, OS characteristics, VM names and tags, the presence of a virus, etc. NSX automatically assigns the appropriate security group and policy based on virtualization relevant context, rather than just physical topology.

Pre-approved security policies are orchestrated and managed centrally, which reduces rule sprawl and ensures that security is accurately and consistently applied. This new level of automation dramatically reduces the operational complexity and expense of managing security policies across workloads.

Every security team uses a unique combination of network security appliances to meet the needs of their environment. In additional to NSX's distributed firewalling capability, organizations should also leverage the platform to automate advanced network security capabilities available from VMware technology partners.

Network security teams are often challenged to coordinate completely unrelated network security services from multiple vendors in relationship to each other. NSX makes it possible to do this. NSX distributes network services into the vNIC context to form a logical pipeline of services applied to virtual network traffic. Third-party network services can be inserted into this logical pipeline, allowing physical or virtual services to be consumed. Enterprises use NSX to build policies that leverage NSX service insertion, chaining, and steering to drive service execution in the logical pipeline.

Integrated security tools also benefit from the operational model provided by the NSX platform. These integrations dramatically increase provisioning speed, management efficiency, and service quality while maintaining separation of duties between server, network, and security teams.

Advanced security capabilities are available through integrations with Palo Alto Networks, Intel Security, Trend Micro, Symantec, Checkpoint, and several other VMware NSX partners.

Create application-level visibility with modern tools

The hypervisor is ideally and uniquely positioned at the boundary between the physical and virtual worlds. Because the NSX vSwitch sees every packet as it enters and leaves a VM, it provides the highest level of visibility and context. It can also correlate the fluid relationships between applications, virtual networks, physical networks, and more.

The following are some example scenarios that demonstrate NSX's unique monitoring and troubleshooting capabilities:

Real-time summary	Monitoring and troubleshooting	Debugging
An operator can pick any virtual machine's network interface and see a real-time summary of all flows and their state. There's no need to configure full-packet captures to a remote tool and sift through IP addresses looking for the VM.	Every aspect of a virtual network is available through NSX's central CLI and central API. This significantly simplifies monitoring and troubleshooting activities because you no longer need to figure out where in the network to look for a problem. Additionally, there is no need to jump to different consoles to perform troubleshooting.	Every packet is handled in software by the vSwitch, giving you more visibility than in traditional networks. You can create a synthetic transaction without the need to have access to the guest VMs. Traceflow packets can be injected into a forwarding pipeline to allow fine-grained debugging of issues in the data path (e.g., overly restrictive ACL policies).

Operators already use many tools to manage and support the data center infrastructure. They use different tools for monitoring, troubleshooting, and change management activities. With network virtualization the same set of existing tools can be used to get visibility into the logical networks.

Real-time monitoring tools are important in virtualized environments that are constantly changing, where infrastructure and applications move dynamically from server to server, and the network is re-configured automatically.

Process best practice: tools

Identify VMware or third-party tools that give you visibility into the object relationships between virtual and physical compute, storage, and network infrastructure. Correlation across the infrastructure domains helps to quickly narrow the scope of an issue to a particular domain, and reduce the need to have multiple domain-specific tools.

The best options are typically modern tools, such as vRealize Operations, Arkin, Riverbed, and others, which are specifically designed for virtual and physical environments. These tools provide an end-to-end view of topology, application health, utilization, and capacity.

Keep in mind that a single-vendor approach may not always give you the best visibility. Multiple tools may be best for optimal monitoring, alerting, and troubleshooting, as is the case today for your physical network. For example, you are likely using different tools for traffic flow analysis (e.g., SolarWinds, NetQoS), packet analysis (e.g., Wireshark, SteelCentral), and alerting (e.g., Netcool, OpenNMS).

Virtual networks provide the same level of instrumentation as in the physical network via standard protocols (e.g., packet and byte stats through SNMP and APIs, SPAN/ L3 SPAN, NetFlow/IPFIX, port mirroring, and Syslog). This allows organizations to get started with their existing monitoring, alerting, and troubleshooting tools, and later transition to a modern tool, such as those mentioned earlier.

Final word on processes

Network virtualization and NSX give you a great reason to assess how you're doing things today—and define a better, more efficient way to move forward. Fixing all processes feels daunting: take an incremental approach to automating your processes to avoid paralysis. Lean and continuous improvement methodologies are great ways to move forward.

Technology

In this section we will explore the architectural and infrastructure considerations when planning, deploying, and operationalizing network virtualization and NSX. Practical use cases around micro-segmentation and disaster recovery will also be discussed.

Design the physical network for simplicity

With NSX the physical network architecture is designed simply for connectivity and performance. That may be as simple as an L2 fabric that you're already using today, or an L3 fabric based on a leaf-spine architecture. You can start with the former and gradually move to the later.

NSX does not impose hard requirements on where L2 boundaries are drawn. Configuration changes to the physical network should be relatively infrequent because it just provides connectivity among hosts. This helps to avoid manual configuration errors.

Decoupling of network services and topologies from physical hardware has enabled L3 spine-leaf fabrics to become widespread. This allows you to establish a common platform with the same logical networking, security, and management model.

By abstracting the virtual network topology, as seen by VMs, from the physical topology, NSX makes a change in network architecture more feasible. NSX frees network designers to more easily move to spine-leaf architectures that use L3 routing with non-blocking ECMP between top-of-rack switches.

The underlying physical network is free to evolve independently of the virtual network, and its architecture is designed around criteria of scalability, throughput, and robustness. Single device or link failure doesn't affect application connectivity.

The ECMP L3 fabric design offers configuration uniformity and enhances device interoperability. Hardware upgrades (e.g., deployment of new switches) can be decoupled from NSX, avoiding impact to workloads running on your virtual networks. NSX supports switches from any vendor, and they can be interconnected together.

Network virtualization overlays combined with spine-leaf architectures lead to greater resiliency and operational efficiency, more efficient use of bandwidth, and scalability to handle the ever-increasing amount of east-west communication inside the data center. While smaller L2 broadcast domains increase the stability of the network.

Implement network virtualization incrementally

NSX network virtualization is not an all-or-nothing proposition. NSX virtual networks do not require changes to the underlying physical network. Network virtualization can transparently co-exist with existing application deployments on the physical network.

Technology organizations have the flexibility to virtualize portions of the network by simply adding hypervisor nodes to the NSX platform. In addition, NSX software gateways or top-of-rack switches (i.e., hardware from VMware partners) deliver the ability to seamlessly interconnect virtual and physical networks. These can be used to support Internet access by workloads connected to virtual networks, or to directly connect legacy VLANs and bare metal workloads to virtual networks.

Technology best practice: start with a single project

You should rollout network virtualization and security incrementally. We recommend that you start with a single use case and set of applications. Identify workloads with an attractive risk/reward profile to leverage new capabilities. For your first implementation, choose workloads that are lower in risk, but that have enough complexity for the purpose of validating NSX in your environment.

The use case you choose to implement will largely determine which NSX functional services you will automate for your virtual networks. For example, if you are automating network provisioning, you may start with logical L2 switching, L3 routing, and edge services. If you are implementing micro-segmentation, you will start with logical firewalling.

Define a strategy and method to continually rollout new NSX features and functionality for your customers. Establish a regular cadence, one that the business knows is coming and can count on for their projects. You will find that regular releases help to increase user engagement, up-take of the services, and customer satisfaction. Allow for organic up-take of the services, rather than trying to artificially force widespread adoption.

Technology best practice: workshops

Staying engaged with business and technology peers in your organization is a great way to ensure the success of any initiative, including network virtualization. Consider holding periodic workshops with users intended to inform and educate stakeholders about the available network virtualization and security services, and update them on your roadmap plans. Encourage application and infrastructure owners to collaborate by providing requirements for future releases as well as feedback on capabilities already available in production.

Use Case: segment around application boundaries

One of the main use cases most NSX customers implement and operationalize early on is micro-segmentation. Micro-segmentation has been considered a best practice security architecture for a long time. When attackers get unauthorized access into the network, segmentation can help limit their movement and prevent a data breach. Micro-segmentation, however, did not achieve widespread use in the past. This was due to architectural limitations in traditional physical networks that make it difficult to operationalize.

NSX makes micro-segmentation operationally feasible. The platform delivers native isolation and segmentation. Advanced services insertion allows third-party security appliances to leverage the NSX operational model.

Isolation is the foundation of most network security, whether for compliance, containment, or simply keeping development, test, and production environments from interacting. Virtual networks are isolated from other virtual networks and from the underlying physical network by default, unless specifically connected together. Operators do not need to deal with physical subnets, VLANs, ACLs, and firewall rules.

Segmentation is related to isolation, but applied to tiers within a multi-tier virtual network. Traditionally, network segmentation is a function of a physical firewall or router, and is designed to allow or deny traffic between network segments or tiers. For example, routers and firewalls segment traffic between a Web tier, application tier, and database tier.

Today's challenges: traditional processes for configuring segmentation are manual, time-consuming, and prone to human error—which can result in security breaches. Implementation requires specific expertise in device configuration syntax, network addressing, application ports, and protocols.

Network virtualization solution: with NSX security policy is applied in the virtualization layer. You can throw away the east-west traffic detouring bag of tricks. Security is applied transparently before packets even arrive at the first virtual network port. Having already been secured at the onset, latency sensitive east-west traffic is free to travel directly to its destination, taking the lowest latency path.

The combination of centralized control with distributed implementation of services means that very fine-grained policies can be applied to every virtual interface in an operationally feasible way. For example, VMs in the same tier of a three-tier app can talk to other tiers, but not to each other. In effect, each workload is wrapped with its own security.

NSX allows you to set security policies based on high-level business constructs (e.g. application, user, or group) rather than low level infrastructure constructs (e.g., IP address, application ports, and protocols). Security policies can be applied with higher precision, accuracy, and alignment to corporate policy—without human interpretation.

Design for workload mobility and recoverability

Traditionally, physical network topologies and address space required IT to change IP addresses when applications were moved. In some cases, IP addresses are hardcoded into applications, which is even more costly because code changes and regression testing are required.

NSX frees your workloads from VLANs and IP addressing, and enables unrestricted workload mobility and placement across the data center fabric. With NSX, workload placement is not dependent on the physical topology and availability of physical network services in a given location.

Everything a VM needs from a networking perspective is provided to it by NSX, wherever it physically

resides. Workloads can freely move across subnets, availability zones, or data centers—without operations having to re-IP them. If a workload is moved, all of its network and security services automatically move with it—with no human intervention.

Organizations use NSX workload mobility and placement to do things like:

- Provision applications faster
- Migrate workloads to a new data center
- Update or refresh the underlying physical infrastructure

Use Case: improving server resource utilization with network virtualization

Organizations are also using NSX to access server capacity available at other locations in the data center or another data center. This allows for substantially greater server resource utilization and consolidation. All of these use cases significantly reduce operational cost and improve agility—and add to the overall value of your network virtualization and NSX investment.

In traditional network topologies each cluster or pod has its own server capacity. Re-configuring the network to access it from another pod or cluster takes too long and is prone to human error. Available server capacity goes to waste. We sometimes refer to this as “dark server capacity” because it’s not easily reachable. In effect, the complexity of traditional network topologies and equipment limit the Technology Organization’s ability to better use available server capacity.

NSX allows you to stretch the network to access capacity available anywhere in the data center. Without touching your existing physical infrastructure. If you want to add another VM, say on a server in a different subnet or availability zone, just bring up the VM and connect it to your logical switch. Those two workloads are now L2 adjacent, even though they are going across multiple subnets and availability zones on the physical network.

Use Case: Disaster recovery

You can also use NSX to complement existing disaster recovery solutions. With the traditional approach to networking, utilizing a back-up site for disaster recovery requires striking a balance between cost and capabilities. Rather than faithfully reproducing their network topology and services in a second location, most organizations opt for a “good enough” solution. Tradeoffs are made to reduce costs, which translates into diminished capabilities relative to their primary data center.

NSX enables zero-compromise disaster recovery. Rather than just taking snapshots of virtual machines, NSX allows you to take a snapshot of the complete application architecture—including networking and security. Ship a copy off to a disaster recovery site where it remains on standby—on any hardware and without any fall-off in functionality.

In the event of a disaster, spin up the VM and you’re done. The network it is expecting to connect to is already running at the recovery site. You significantly reduce your recovery time objective because you don’t have to re-configure the workloads and security appliances with new IP addresses.

Final thought on technology considerations

Network virtualization and NSX offer a tremendous amount of new flexibility for your technology environment. It unlocks a number of valuable use cases. Rather than getting overwhelmed with all of the

possibilities, first focus initially on service quality. Expand the footprint of your initial use case. Then choose a second use case to operationalize. Deliver new capabilities only after your team and users are happy with the quality levels.

Next Steps

Operationalizing network virtualization and security should be viewed as a journey. One where your organization achieves ever-growing maturity and sophistication as you move toward the software-defined data center and deliver increased value to the business.

Your organization and individual team members have a variety of options available to learn more about how to achieve the full operational benefits available with network virtualization and NSX, and how it fits with and complements the rest of your IT organization.

Step one: learning

A great first step is providing learning opportunities for your organization and individuals. Combine different types of education and learning: both formal (e.g., workshops, courses, hands-on labs, programs) and informal (e.g., lunch and learns, coaching, mentoring). In order to incentivize learning, consider ways to include training and learning objectives in personal MBOs.

To get started, your team can participate in VMware's hands-on labs (labs.hol.vmware.com), and instructor-led workshops and courses available through VMware Education (vmware.com/education). VMware also provides NSX operations guides focused on monitoring and troubleshooting.

Step two: transformation services

Getting an outside perspective to help with your transition to network virtualization and NSX can significantly accelerate the process. VMware provides Operations Transformation services and workshops (vmware.com/consulting). For example, Network as a Service (NaaS) Envisioning helps you to clearly identify the vision, goals, and objectives of your new network and security operating model. NaaS Discovery helps you to identify which operational and organizational capabilities you need to enhance or create to realize the new operating model and achieve the expected goals and outcomes.

Step three: simple pilot

One of the best ways to learn NSX and see how it can be operationalized is to start a production pilot with a single use case and a few workloads. Choose workloads that are lower in risk, but that have enough complexity for you to maximize learning about how NSX is operationalized.

Contact your VMware or partner account executive to help you get started.

Appendix

End-state performance characteristics

The following table summarizes the NSX operationalization end state characteristics for people, process, and technology. You can use this as a guide for your journey:

Vector	Current/Beginning State	Future/Ending State
Org Structure	• Siloed with rigid boundaries that necessitate heavy processes • Formal request procedures • Throw it over the wall • Finger pointing: us vs. them • Different and misaligned goals, objectives, and incentives	• Blended with immediate interactions • Open communication • Condensed feedback loops • Highly collaborative • Shared goals and KPIs • Shared risks and responsibility
People	• Specialization • Expertise limited to a domain • Use of CLIs and Scripts • Widely available knowledge • Limited career growth • Hardware Infrastructure-centric	• Cross-domain and disciplinary • Multiple domain expertise • Use of APIs and automation tools • Continuous learning • Opportunity to make business impact through strategic projects • Service and application-centric
Processes	• Manual and error-prone • Cumbersome ticketing systems • Coordination and hand-offs • Complexity and bottlenecks • Waiting for service • High OpEx • Infrastructure focused	• Automated, standardized, consistent, and auditable • Low risk from manual errors • Fast turnaround/SLA-backed • Real-time interactions • Reduced OpEx • Service or application focused
Tooling	• Legacy, domain-specific • Siloed and multiple tools • Physical only instrumentation • Infrastructure focused • Difficult to isolate service issues • Individual component CLIs	• Modern, cross-domain tools • Designed for virtual and physical instrumentation • Application focused • Integrated infrastructure and service monitoring • Easy to isolate service issues • Centralized CLIs and APIs to instrument infrastructure

Vector	Current/Beginning State	Future/Ending State
Architecture	• Classic 3-tier architectural limitations • Workload shackles • Chokepoint firewalls • Oversubscribed core • Link performance • Centralized, location-bound services	• Spine-leaf fabric with non-blocking ECMP • Overlay with decoupling and abstraction • Workload portability and mobility • Native isolation and segmentation • Scalability and resiliency • Distributed services
Infrastructure	• Physical with slow changes in underlay • Infrastructure-bound security • Diminished, “good enough” DR • Human interpretation of policy • Infrastructure-centric policies • Low-level infrastructure constructs • Fragmented management • Hardware vendor lock-in • Difficult to do service chaining	• Virtual with dynamic changes in overlay • Application-focused security • Zero-compromise DR • Machine readable security policies • Business-centric policies • High-level business constructs • Centralized management • Price/performance choice • Easy to do service chaining

Cloud networking and security roles

The following descriptions will help you define the roles and responsibilities of cloud networking and security staff. These cloud roles are performed by “traditional” network and security professionals; i.e., by people you already have on your teams.

In small or medium-sized businesses it is common for a single person to perform two or more of these roles. For example, a single network engineer may be responsible for network architecture, development, and/or operations. Not all organizations will need to have a different person(s) in each of these roles.

On the other end of the spectrum, it is quite common for large enterprise to have multiple people doing the same/similar role. For example, we’ve seen many multi-national companies that have several cloud network architects or cloud network engineers.

Cloud Networking Roles

The *Cloud Network Architect (CNA)* is responsible for developing end-to-end cloud network architectures and standards according to a service-based consumption model (Network-as-a-Service). The CNA performs the following responsibilities:

- Determines technical and operational network requirements
- Designs physical and logical networks that address application requirements (e.g., capacity and performance)
- Develops and validates tests to ensure that requirements are addressed
- Guides the planning and implementation of cloud network solutions

The *Cloud Network Engineer (CNE)* is responsible for low-level design of network services and infrastructure, development and testing of the network functions, provisioning of capacity, and definition of the network configuration. The CNE performs the following responsibilities:

- Ensures fulfillment of customer requirements and related service levels

- Translates requirements into logical blueprints and configuration templates
- Designs, develops, and tests custom workflows and scripts for routine tasks (e.g., integration, deployment, monitoring, and compliance)
- Provides troubleshooting assistance to level 2 and 3 support, and proposes solutions and requests fixes

The *Cloud Network Operator (CNO)* has overall responsibility for all facets of Day 2 operations, fulfilling application operational requirements (e.g., performance and capacity), and maintaining the cloud network infrastructure, tooling, and platforms. The CNO performs the following responsibilities:

- Executes and controls automation for provisioning, management, monitoring, alerting, and troubleshooting
- Proactively monitors the cloud network infrastructure, and takes action on events before they affect service
- Performs troubleshooting, root cause analysis, and applies solutions and fixes proposed by the CNE
- Provides level 2 and 3 support, and manages incidents, problems, and escalations

Cloud Security Roles

The *Cloud Security Architect (CSA)* has overall responsibility for all facets of architecting, designing, and supporting the cloud security infrastructure. Across network security virtualization, automation, orchestration, and monitoring. The CSA performs the following responsibilities:

- Assesses security risk for cloud infrastructure and applications, and provides authoritative guidance on security strategies and solutions
- Determines technical security policies, processes, and audit capabilities required to address cloud security requirements and goals
- Develops validation tests to verify cloud security solutions, and plans and guides their implementation
- Maintains a thorough knowledge of threats and risk mitigation strategies

The *Cloud Security Engineer (CSE)* is responsible for translating security policies into security controls that can be audited. The CSE performs the following responsibilities:

- Designs and implements physical and logical solutions that realize cloud security controls
- Orchestrates and automates cloud security processes (controlling, monitoring, and auditing)
- Integrates and implements cloud security services and tools that fulfill requirements and service levels
- Engages in escalations, investigates breaches, and recommend and implements remediation solutions

The *Cloud Security Operator (CSO)* is responsible for understanding, implementing, enforcing, verifying, and maintaining specific security controls as required by organizational policy and risk assessment. The CSO performs the following responsibilities:

- Monitors, detects, and analyzes security anomalies, vulnerabilities, and threats
- Manages security logs, ensures compliance with logging standards, and assists in security audits
- Investigates, diagnoses, and resolves cloud security issues in response to incidents
- Implements security solutions and fixes for vulnerabilities

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com