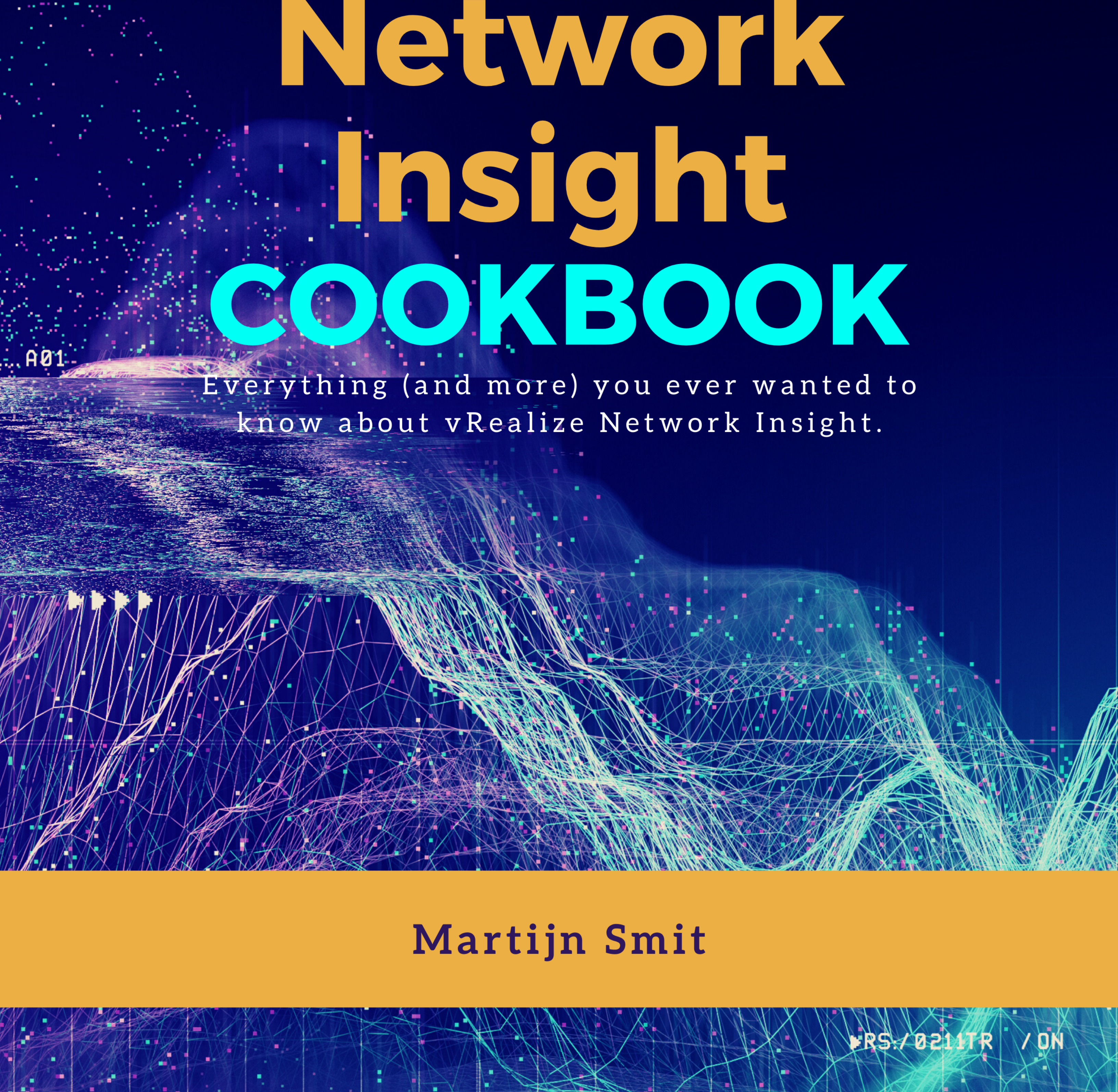
vRealize Network Insight

COOKBOOK

Everything (and more) you ever wanted to know about vRealize Network Insight.



Martijn Smit

vRealize Network Insight Cookbook

Everything (and more) you ever wanted to know about vRealize Network Insight.

Martijn Smit

This book is for sale at http://leanpub.com/networkinsight

This version was published on 2020-06-01

Contents

Introduction

Thank you for purchasing the vRealize Network Insight Cookbook! This book is for people in jobs or interests related to networking and security in private, hybrid, and public clouds. Managing these networks and security policies becomes a much easier job with Network Insight, and this book will try to explain best how to go about managing those networks and how Network Insight itself is positioned to do so.

Sometimes it's not all in the name. This is also true for vRealize Network Insight, as it gives you not just insight into your network, but your compute, storage, and network layers.

> While the full product name is VMware vRealize® Network Insight™ and VMware vRealize® Network Insight™ Cloud for the Software-as-a-Service version; please note that I'll be using the shorthand 'Network Insight' from now on.

With Network Insight, you can take the guesswork out of deploying micro-segmentation with comprehensive network flow analytics to map out real-time traffic and model security groups and firewall rules to successfully implement micro-segmentation security policies. It also helps to improve the performance and availability of the infrastructure by combining and correlating virtual and physical compute, storage, and networking components to provide a clear and full picture of the infrastructure.

It does not discriminate between virtual machines or physical servers, provides detailed information about the smallest workloads (containers), has integrations with the VMware Virtual Cloud Network vision and everything that runs beneath the Virtual Cloud Network.

Network Insight collects data from data sources like VMware vSphere, VMware NSX, Physical network devices (switches, routers, load balancers, and firewalls), Physical converged systems, IPAM systems, and log collectors. All this information is put in a structured database, correlated, and available via the intuitive user interface and API. The way this converged information is presented in the user interface is what makes Network Insight unique and such a pleasure to work with.

It's all about the fundamentals of the platform, as it's designed from the ground up to be as open as possible. This means you can retrieve any, and all the data that is gathered and do all kinds of neat things with it like filtering, grouping, sorting, and perform other modifiers on it (more on that in the chapter Using the Search Engine.

Apart from configuration and operational data, you can also send real-time network flow (NetFlow or sFlow) data to Network Insight to map out which workloads in your environment talk to each other. Because all data is correlated, the network flow data is linked to the source or destination workload (virtual machine or physical host), and you can see the name of the workload related to the flow, instead of just seeing that **10.0.0.10** talks to **10.0.1.11** over port **80**.

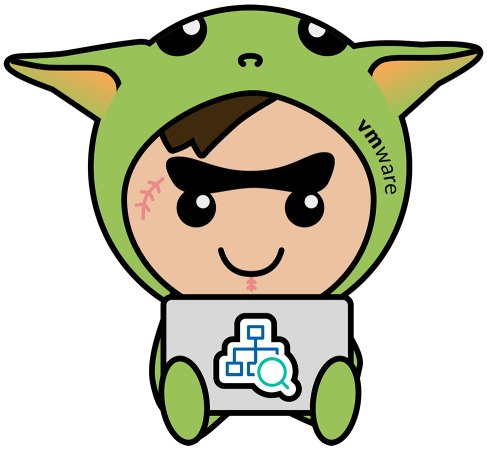
> ℹ **Configuration data** is meant as the configuration of the data source (i.e., show running-configuration on a physical Cisco device and the inventory of a VMware vCenter, etc.). **Operational data** is meant as dynamic, changing data on data sources (i.e., the route and mac tables on a network device, IP addresses of virtual machines, etc.).

This network flow data is typically generated by the vSphere Distributed Switch, the NSX Distributed Firewall components, or a physical network device.

Due to the technical and sometimes very specific nature of this book, it's advised to have a Network Insight instance ready to go while you are reading; so, you can try things out with data from your infrastructure!

The content of this book is based on Network Insight 5.0 (with some small nuggets on 5.1 because I took too long to write it). Considering the product team is an innovation engine and moves really quickly (delivers major features every three months), you need to doublecheck the details when you're using a newer version. This book also does not intend to replace the official documentation[1], but rather complement it. The specific technical details in this book will age, and rightly so.

[1] https://docs.vmware.com/en/VMware-vRealize-Network-Insight/index.html



Meet Fred, the vRealize Network Insight Mascot

How to Use This Book

As the book title suggests, this book acts as a cookbook for Network Insight. It will provide context and background information on the Network Insight features, and explain how to use them. I hope that you can use it for two goals:

1. Use the book to get you started with learning Network Insight if you're new to the product.
2. Use it as a reference guide while working with Network Insight in your day to day operations.

There is a ton of technical information here, including automation code, call out tips and tricks, key points, and more. To make sure you get the most out of it, I'd like to cover a few conventions that I'll use in this book.

Bold
Used for essential bits of information that will come back in the following text, or that is referenced in an image.

Links
Throughout this book, there will be links to external resources, but also internal links to other chapters. Although I've tried to keep each chapter standing on its own, there will be call outs to previous chapters to refresh your memory.

> This is a call-out box. It'll contain either a tip or trick based on the previous text or an important call-out to summarize the previous text. In any case, I'd like you to remember these call-outs.

> This is a 'key tip' call-out box. It'll contain a descriptive way to access a 'hidden' feature of Network Insight.

Search queries
There are many search query examples throughout this book. These search queries look like this:

```
VMs where vCenter = myvc
```

Command Prompt Output
Executing commands on Network Insight, or executing an automation script has output. To show examples of these outputs, there are some command prompt outputs throughout this book. Here's an example:

```
PS ~/> ./example.ps1
Counting from 1 to 9 (in seconds):  1 2 3 4 5 6 7 8 9
PS ~/>
```

Code Examples

Mostly confined to the Automating Network Insight chapter, there will also be example code. Here's how that will look:

```
x = 1
if x == 1:
  # indented four spaces
  print("x is 1.")
```

Foreword by Shiv Agarwal

Founder of ArkinNet, currently VP and GM of vRealize Network Insight with VMware

VMware vRealize Network Insight (or vRNI, or Network Insight) has seen massive adoption in VMware's' customer base, helping our customers get end-to-end visibility and operational simplicity as they embrace a software-defined approach to networking and security. Network Insight completes VMware's Virtual Cloud Network vision and story by providing seamless visibility and converged network operations across the data center (virtual and physical) and hybrid cloud as well as branch offices and remote sites (via SD-WAN integration).

Jogging down the memory lane, Network Insight came into VMware through the Arkin (ArkinNet) acquisition. As it happens so often in Silicon Valley, my co-founder and I were at VMware before we went out and started Arkin (in 2013). We had joined VMware (in 2008) as part of the Blue Lane acquisition. At Blue Lane, we had built a virtual firewall which became the first-generation virtual firewall (VMware NSX DFW) inside VMware. During our first tenure at VMware (2008-2013), NSX was in its infancy.

We saw enterprise customers struggling to operate their virtual networking stack. They were trying to use their existing legacy processes and toolset. Their people's mindset was geared and tuned to managing physical networks. Virtualization was new to the network operators. That's when my co-founder and I got the idea of starting Arkin. You start a company with a big vision, and ours was to transform how networks are operated. The idea was to bring consumer-grade simplicity to managing networks. We wanted to challenge the status quo.

Our first set of use cases was to help customers implement micro-segmentation and operationalize NSX. NSX was becoming the dominant network virtualization stack, and we betted on it. We got the first product out in 18 months with some of the marquee NSX customers using it in production and were acquired by VMware in 36 months. At VMware, it was like a match made in heaven. Thanks to the NSX sales team, the two products together (NSX and Network Insight) started flying off the shelf! It's been fun! I tell my team often that the acquisition by VMware was a little pit stop in our journey, which, at the time of writing this foreword, is continuing.

We continue to build. Network Insights expanded charter and scope now includes end-to-end network operations - monitoring, troubleshooting, and optimization. By combining the different types of network data (flows, metrics, config, and more), we have provided a unique platform for our customers to converge their traditionally silo-ed visibility and realize a multitude of use cases around next-generation networking and security. We have also created a unique advantage for ourselves by adding a strong application context to network and security datasets. Applications are the lifeline of an enterprise, and Network Insight's powerful application discovery and planning feature enables our customers to see their network and security data through the lens of their applications. We are thus elevating IT and empowering them to have a more business-oriented conversation with their line of businesses.

Over the next few years, we see the operational silos breaking at a rapid pace and a lot of automation happening, ultimately leading to self-driving networks. That's the future. Silos create inefficiency and finger-pointing. Our vision is to bring a high degree of efficiency in network operations through convergence, consumer-grade experience, and analytical insights. We continue to deliver upon our vision by investing in new areas. Recently, we acquired a company, Veriflow, which has pioneered the area of network verification in software. This technique is used in many mission-critical industries where failure can be catastrophic such as airlines and space. Networking is mission-critical for our customers. With this acquisition, we are arming our customers with network modeling and prediction and significantly push the frontier of network operations in the enterprises.

I am thrilled and excited to be writing this foreword for Martijn's book on VMware vRealize Network Insight. Martijn has been the technical face and flag bearer of Network Insight in the EMEA region for a long time, even since before the acquisition. I hope the insights captured in this book triggers a genuine thought about transforming their network and security operations in the mind of its readers.

About the Author

The first thought going through my head, after decided to write this book, is: why? Why on earth are you starting another big project that's going to take up a ton of time? The reason is simple: Hi, I'm Martijn Smit, and I'm an information-sharing addict (echo's: "hi Martijn!").

I'm proud to be Dutch and proud to be in the IT industry. My career started at a hosting company, in which I spent eight years moving from the web hosting help desk to colocation & dedicated server support to managing the internet-network and helping to build a new datacenter from the ground up. After this provider, I joined an integrator company, with which I spent five years designing and deploying data center infrastructures, including storage, compute, networking, and virtualization. I was also in the innovation group that brought the last two together to support virtual networking; Software-Defined Networking (SDN).

I currently work at VMware in Technical Marketing for vRealize Network Insight, as I wholeheartedly believe in the way Network Insight approaches network troubleshooting and monitoring and want to spread the word. My previous role was to guide customers to the world of virtual networking as a Networking & Security Solutions Engineer.

Apart from my passion for technology, I believe in a healthy balance and taking care of yourself, so often take 2 to 3-hour bike rides, exercise every day, and (try to) eat proper food. One of my favorite hobbies is spending time doing slow cooks on my Kamado barbecue. I also tear through books and have a goal to read at least 30 books yearly. I'm an information-sharing addict and mostly do so by giving talks and doing technical blogs. If you would like to see more of my rants, you can follow me on twitter on @smitmartijn[13] or my blog at https://lostdomain.org

Back to this book; so, I have been dealing with the entire data center stack for years. One of the things that always annoyed me was that there was no right solution to troubleshoot and monitor that entire stack; it was still separate solutions for each layer. In 2014, I came across a company called ArkinNet, which had a fantastic product which could collect data from multiple layers (storage, compute, and networking) and holistically present it. After doing some due diligence, I immediately included Arkin into our product portfolio, and I've been in love with the product ever since.

ArkinNet was later acquired in June of 2016 by VMware, and it is now known as vRealize Network Insight.

[13] https://twitter.com/smitmartijn

Introduction to Network Insight

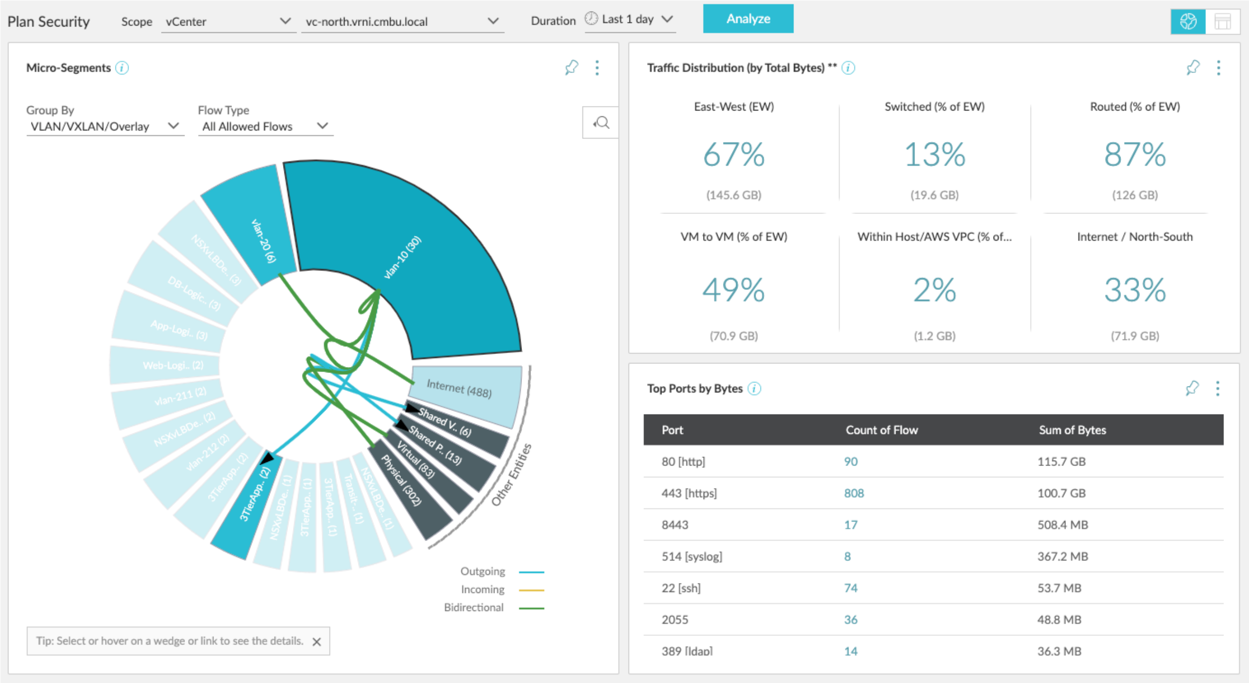
Due to the vast amount of data that Network Insight has, and the range of that data (i.e., network flows, switch port metrics, VMs, AWS inventory, and much more), the actual use cases for Network Insight are limitless. Four main use cases help you to get an idea of what to use Network Insight for. In the following chapters, I'll discuss the **why** of using Network Insight. Most of the remainder of this book is the **how** to use it.

Application Security Planning (Micro-segmentation)

Security in the data center is evolving, and micro-segmentation is a technique that is used more and more. You can write an entire book about the technique and technology behind it, but I'll give you a quick summary in chapter Application Security Planning when we go into the depths of the micro-segmentation planner.

The hard part about micro-segmentation is where to get started. As a security person, you need a lot more information about the workloads then you usually get from the application team or vendor, to properly perform micro-segmentation.

Using the network flow data and workload information that is collected by Network Insight, it provides you with a jumping board to accelerate any micro-segmentation implementation. You'll get unobstructed views into the communication between workloads and applications, and you can export recommended security policies that you can import directly into VMware NSX.



Scope: vCenter, vc-north.vrni.cmbu.local

Duration: Last 1 day

Group By: VLAN/VXLAN/Overlay

Flow Type: All Allowed Flows

Traffic Distribution (by Total Bytes) **

East-West (EW): 67% (145.6 GB)

Switched (% of EW): 13% (19.6 GB)

Routed (% of EW): 87% (126 GB)

VM to VM (% of EW): 49% (70.9 GB)

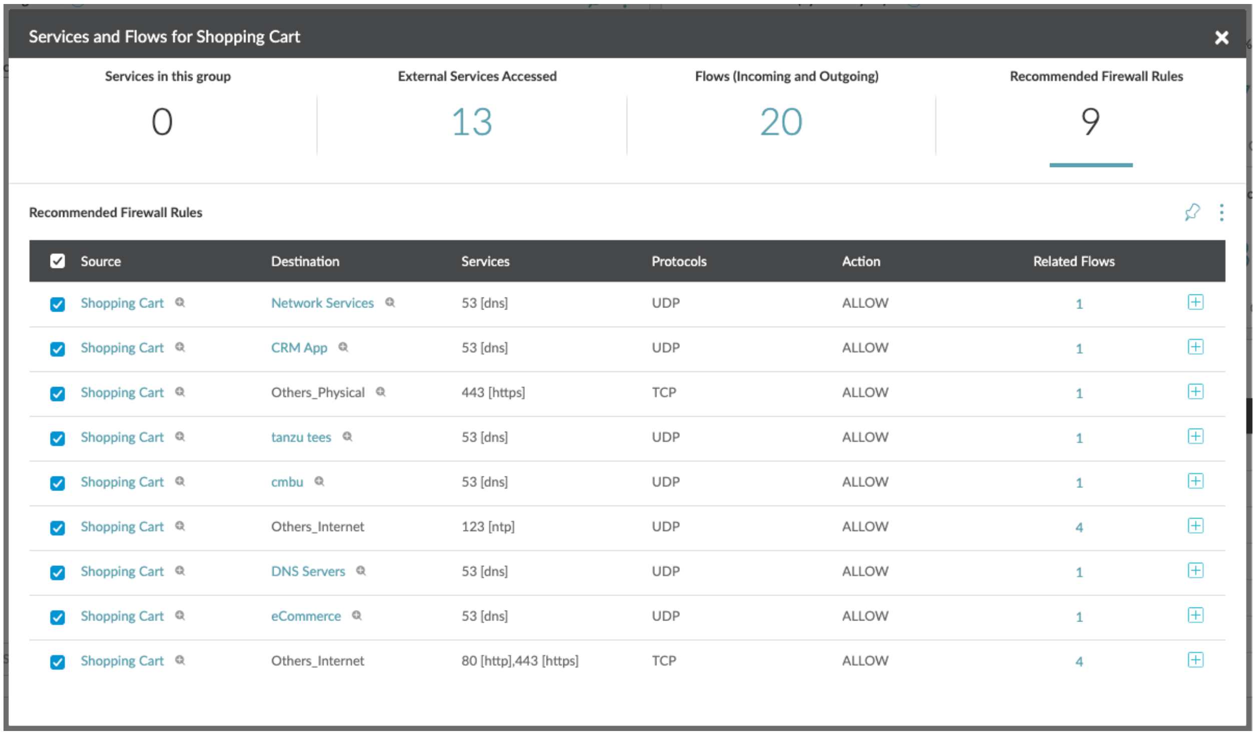
Within Host/AWS VPC (% of...: 2% (1.2 GB)

Internet / North-South: 33% (71.9 GB)

Top Ports by Bytes

Port	Count of Flow	Sum of Bytes
80 [http]	90	115.7 GB
443 [https]	808	100.7 GB
8443	17	508.4 MB
514 [syslog]	8	367.2 MB
22 [ssh]	74	53.7 MB
2055	36	48.8 MB
389 [ldap]	14	36.3 MB

Network Traffic Behavior



Services and Flows for Shopping Cart

Services in this group	External Services Accessed	Flows (Incoming and Outgoing)	Recommended Firewall Rules
0	13	20	9

Recommended Firewall Rules

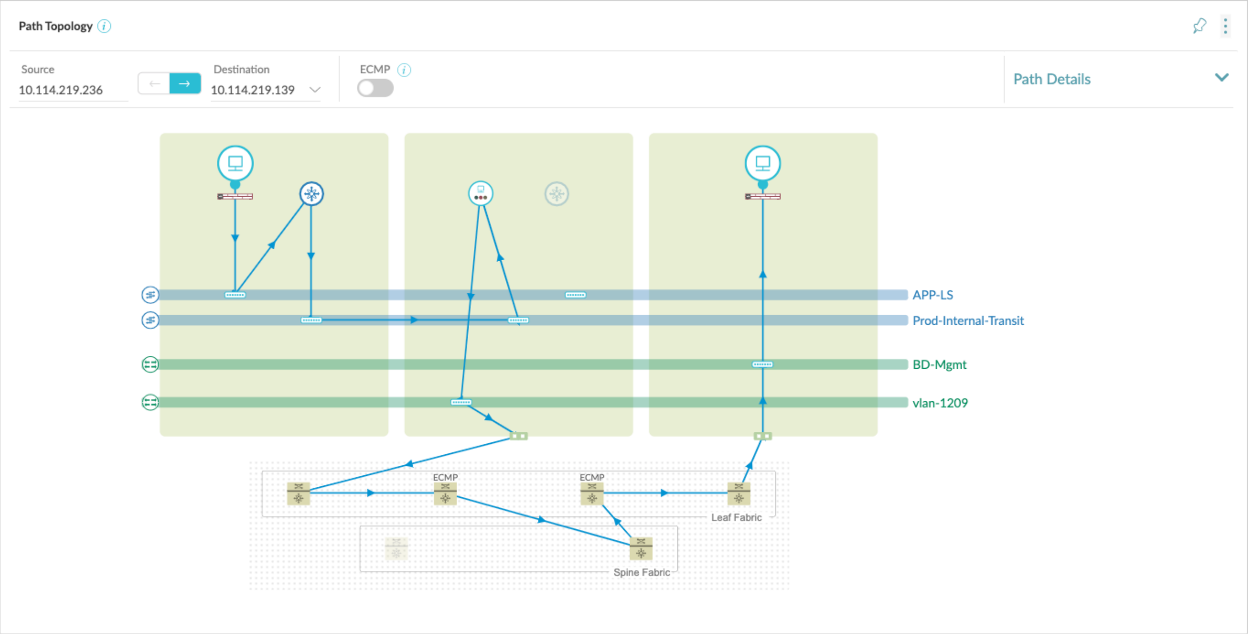
☑ Source	Destination	Services	Protocols	Action	Related Flows
☑ Shopping Cart	Network Services	53 [dns]	UDP	ALLOW	1
☑ Shopping Cart	CRM App	53 [dns]	UDP	ALLOW	1
☑ Shopping Cart	Others_Physical	443 [https]	TCP	ALLOW	1
☑ Shopping Cart	tanzu tees	53 [dns]	UDP	ALLOW	1
☑ Shopping Cart	cmbu	53 [dns]	UDP	ALLOW	1
☑ Shopping Cart	Others_Internet	123 [ntp]	UDP	ALLOW	4
☑ Shopping Cart	DNS Servers	53 [dns]	UDP	ALLOW	1
☑ Shopping Cart	eCommerce	53 [dns]	UDP	ALLOW	1
☑ Shopping Cart	Others_Internet	80 [http],443 [https]	TCP	ALLOW	4

Recommended Firewall Rules Grouped by Application

Getting actual visibility into your environment

Besides using NetFlow data to provide insight into the traffic going through your network, Network Insight also gathers data from your private cloud running on vSphere, public cloud on AWS, and physical equipment that helps run those environments. It uses all that data to paint a complete picture of your workloads, from a virtual machine to the physical wire between 2 routers to the public cloud instance where your web server is running.

When it comes to troubleshooting, that is where the gold is. Network Insight provides a holistic view of your entire environment, which means you can quickly and easily find root-causes to any issues you're having.



Path Topology

Source: 10.114.219.236

Destination: 10.114.219.139

ECMP

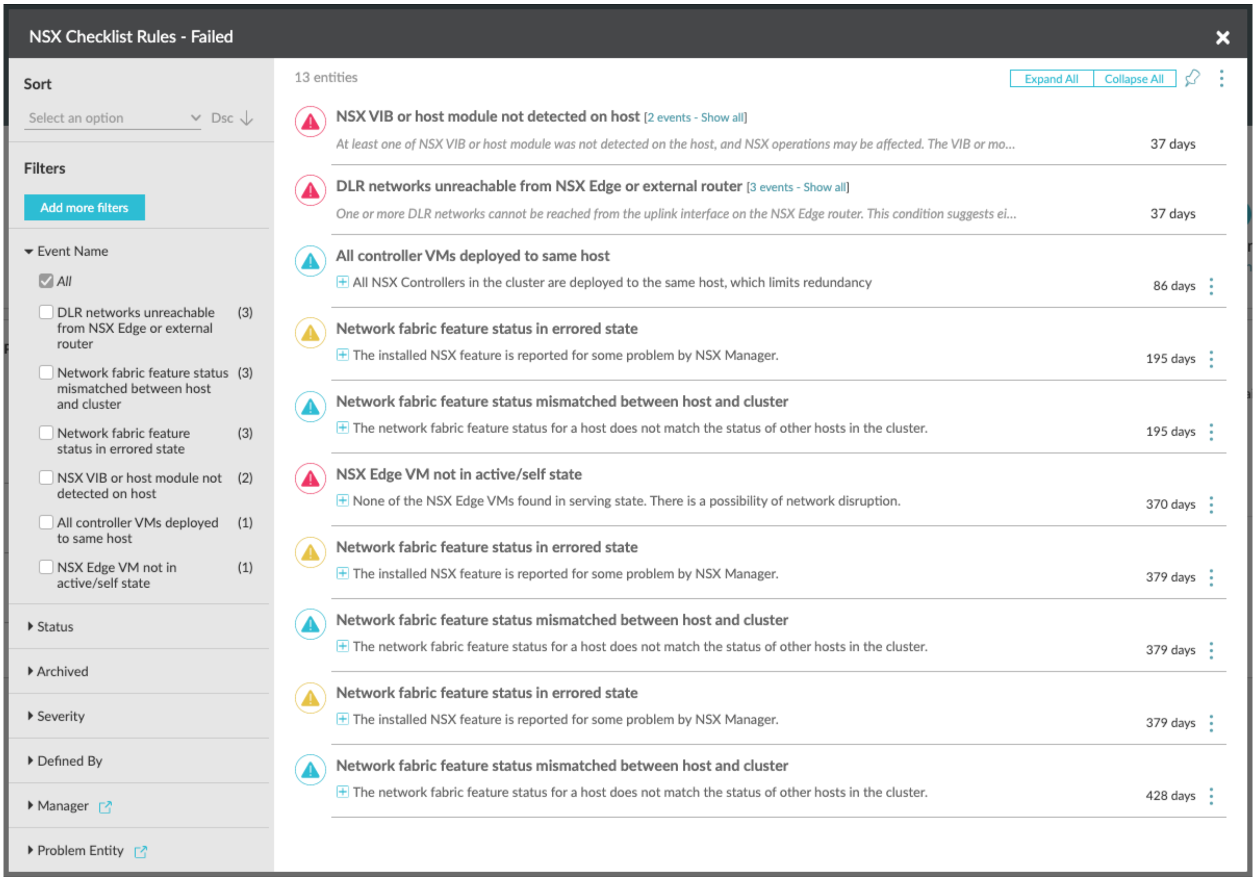
Topology: Physical and Virtual Together

Using the network topology maps, you can quickly determine issues on a specific network path or using the search engine to look for network devices that are misbehaving or showing anomalies, and your troubleshooting process can be much more efficient and quicker.

Doing the Health Check Boogie

After getting all of this data from your virtual and physical environment, Network Insight checks the configuration of virtual and physical devices against the VMware Knowledge Base (KB) and best practices. It provides you with a list of problems in the configuration and ways on how to fix them.

These problems have severities: Critical, Moderate, Warning & Info and example might be that it has discovered an MTU mismatch (essential when using an overlay) on the physical networking equipment or if high availability on an NSX Edge is not enabled. You're at risk for downtime when the NSX Edge needs a failover, which is why Network Insight raises events for this.



NSX Checklist Rules - Failed

Event Name

☑ All

□ DLR networks unreachable from NSX Edge or external router (3)

□ Network fabric feature status mismatched between host and cluster (3)

□ Network fabric feature status in errored state (3)

□ NSX VIB or host module not detected on host (2)

□ All controller VMs deployed to same host (1)

□ NSX Edge VM not in active/self state (1)

13 entities

NSX VIB or host module not detected on host [2 events - Show all]
At least one of NSX VIB or host module was not detected on the host, and NSX operations may be affected. The VIB or mo... 37 days

DLR networks unreachable from NSX Edge or external router [3 events - Show all]
One or more DLR networks cannot be reached from the uplink interface on the NSX Edge router. This condition suggests ei... 37 days

All controller VMs deployed to same host
⊞ All NSX Controllers in the cluster are deployed to the same host, which limits redundancy 86 days

Network fabric feature status in errored state
⊞ The installed NSX feature is reported for some problem by NSX Manager. 195 days

Network fabric feature status mismatched between host and cluster
⊞ The network fabric feature status for a host does not match the status of other hosts in the cluster. 195 days

NSX Edge VM not in active/self state
⊞ None of the NSX Edge VMs found in serving state. There is a possibility of network disruption. 370 days

Network fabric feature status in errored state
⊞ The installed NSX feature is reported for some problem by NSX Manager. 379 days

Network fabric feature status mismatched between host and cluster
⊞ The network fabric feature status for a host does not match the status of other hosts in the cluster. 379 days

Network fabric feature status in errored state
⊞ The installed NSX feature is reported for some problem by NSX Manager. 379 days

Network fabric feature status mismatched between host and cluster
⊞ The network fabric feature status for a host does not match the status of other hosts in the cluster. 428 days

Health Check and Health Alerts

These health checks are an excellent way to keep your environment in check and configured as per the latest best practices.

Migrating to the Cloud (or anywhere)

These days, it's not surprising to have a cloud-first strategy when it comes to developing and deploying new applications. Public Clouds like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform have extensive services that save you a lot of trouble having to build your own. Solidified services like Infrastructure- (workloads), Database-, Storage- and CDN-as-a-Service are making way for services that we are using to kickstart application development. Things like Artificial Intelligence & Machine Learning, Containers, IoT management, facial recognition, forecasting, serverless, are all available as-a-Service so developers can focus on their actual business requirements and churning out code for that purpose. Not be side-tracked by creating their own generic (but mandatory) services that they only need to support their applications and isn't core business.

What does this have to do with Network Insight, you ask? Well, unless your organization is starting from scratch and has no history whatsoever, you're going to have existing infrastructure and applications. In some instances, strategies come into life to use public clouds with Infrastructure-as-a-Service instead of on-premises, and applications are migrating towards the public cloud.

This use-case is also valid for migrations in general, whether it be to the public cloud, to a different on-premises data center, or migrating a piece of your company (for mergers and acquisitions). Any scenario where you have an existing application infrastructure and need to migrate those existing workloads.

Here is where Network Insight can help you map out the application landscape and discover what talks to each other. Applications are usually interconnected, even if they shouldn't be, at all. As it's in the best interest of application performance to keep a grasp on those interconnections, you need to have a proper map of your application landscape.

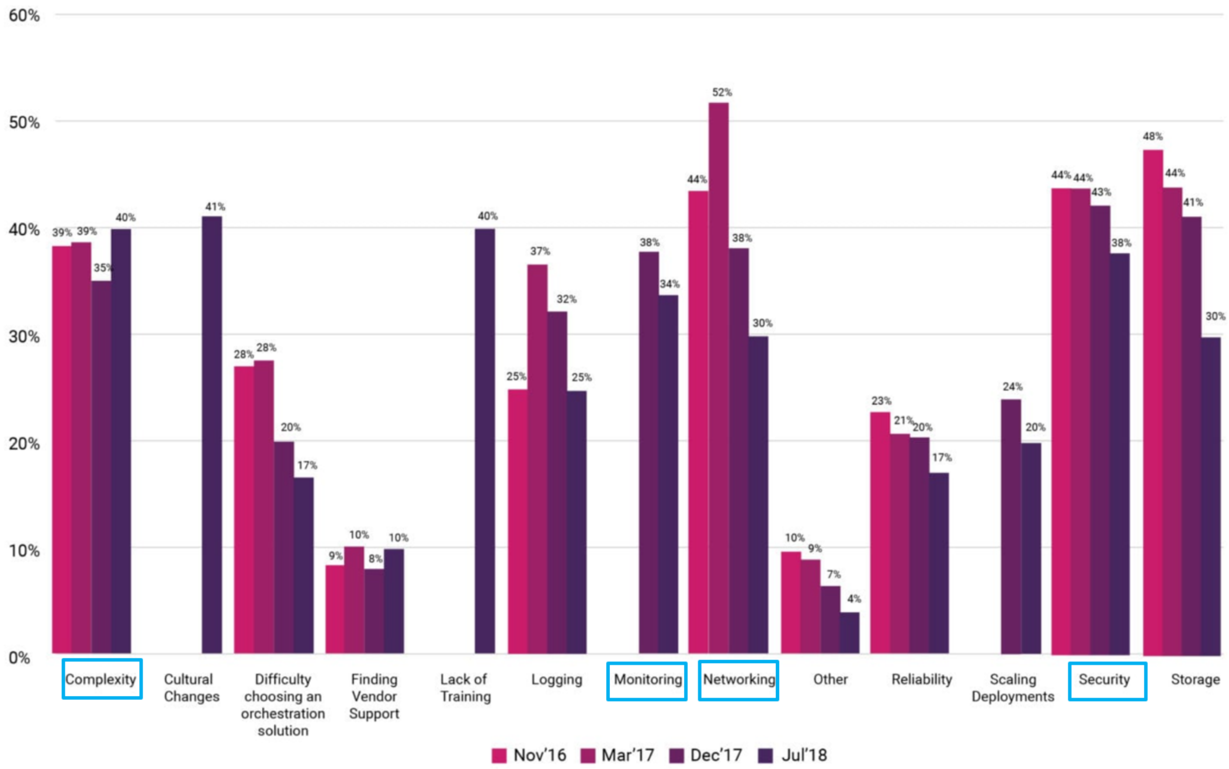
As Network Insight understands application constructs and sees everything that happens on the network, it gives you the map of your application landscape on a silver platter. Besides network data, this map is supplemented by compute and storage performance data to get a handle on the needed resources for the migration. You can then turn around and use this map and plan out your migration.

With a good understanding of the application map, it is much easier to retain application performance when doing migrations.

You can find a deep dive on this topic in the chapter Application Migration Planning.

Visibility for Kubernetes

According to results of a survey that the Cloud Native Containers Foundation did in 2018, the main concerns around moving containerized applications into production (and keeping them there & healthy) is around **Complexity**, **Monitoring**, **Networking** and **Security**.



CNCF 2018 Survey results

[14]

VMware has seen these challenges and is taking them on in several ways. One of those ways is through NSX Data Center for Containers, where network virtualization is delivering simplicity, flexibility, and security up to the container level. Operations engineers can use the same security controls over containers as they can over VMs and make sure the applications are put into production safely – whether the application is hosted on-premises or in the public cloud. That's **Networking** and **Security** covered.

Network Insight comes in to provide clarity of the container environment, reducing the **Complexity** and allows you to **Monitor** this environment for any **Networking**

[14] https://www.cncf.io/blog/2018/08/29/cncf-survey-use-of-cloud-native-technologies-in-production-has-grown-over-200-percent/

and **Security** related events. It does this by making connections between the container world, the virtualized world, and the physical world. In doing so, it creates full end-to-end visibility to make sure the production environment is up to snuff, and no components are acting up.

Network Insight can also be used to plan out the security for these container workloads. Due to the tight integration with NSX Data Center for Containers, Network Insight gains the same network flow visibility as with VMs. This visibility means the same security planner can be used to map out network connectivity between the different levels of the containerized application, and the best part is that Network Insight can generate recommended firewall rules based on those real-time network flows.

Oh, and it also allows exporting these recommended firewall rules in a format that Kubernetes understands (YAML). Applying these rules is as simple as performing the export and using **kubectl** to apply them directly to a running application.

You can find more on how to export the recommended firewall rules in the chapter Application Security Planning.

vRealize Network Insight versus vRealize Network Insight Cloud (SaaS)

When reading about Network Insight, you might come across two versions of the name: vRealize Network Insight (or vRNI) and vRealize Network Insight Cloud (or vRNI Cloud). The reason for this is that there is an on-premises and a software-as-a-service (SaaS) version.

In 2018, VMware came out with a SaaS version, which is lives on their Cloud Services (https://cloud.vmware.com) infrastructure. The reasons for this are to simplify deployments and unburden organizations with upgrades or availability of the platform. VMware takes care of the upgrades, scalability, and availability, and you can simply consume the product. Capability-wise, the 2 are equal; they have the same features and same interface. Everything in this book pertains to both versions.

The architectural components in the on-premises version and SaaS version are similar; they only live in different locations. The chapter Architecture goes deeply into the architecture of both versions, but here's a sneak peek: Network Insight consists out of collector nodes and platform nodes. The collectors talk to your infrastructure endpoints to collect data, and the platform is the central data repository, and it is your entry point (the user-interface).

In the on-premises version, both components run on your infrastructure (which can even be air-gapped), and you keep everything local. With the SaaS version, the collectors run locally (for them to connect to your infrastructure), and they send their data towards the cloud-hosted platform nodes.

The cloud usually brings up 2 security questions; how is the data transferred, and what exactly is stored in the cloud? Stay tuned for details on the transfer in the Architecture chapter, but let's have a look at what data is stored inside the platform.

Collectors look at data center infrastructure components (switches, routers, load balancers & firewalls) configurations. It absorbs things like firewall rules, switch port configurations, virtual workload environments for virtual machines, and, most importantly, network traffic flow data. In this network flow data, source, destination, and protocol are recorded. Of the virtual machines, the metadata is recorded (network settings, hostname, OS type, and more), and cross-linking happens between the different data types. For instance, a network flow can have a VM tagged to it if the VM was either the source or destination of the flow.

The data only contains infrastructure metadata and network flows though, no user or application data from inside the VM is collected. This fact makes it a lot easier to determine whether you could host this metadata in the cloud, as most governmental regulations about data locality pertain to end-user and application data.

If you can make use of the hosted version, it does save you a bunch of management effort by outsourcing that to VMware.

Want to keep learning?

Get the full version on digital at Leanpub.com/networkinsight[1] or get a paperback copy from Amazon[2].

[1] https://leanpub.com/networkinsight
[2] https://amzn.to/3d1CVX7