vmware

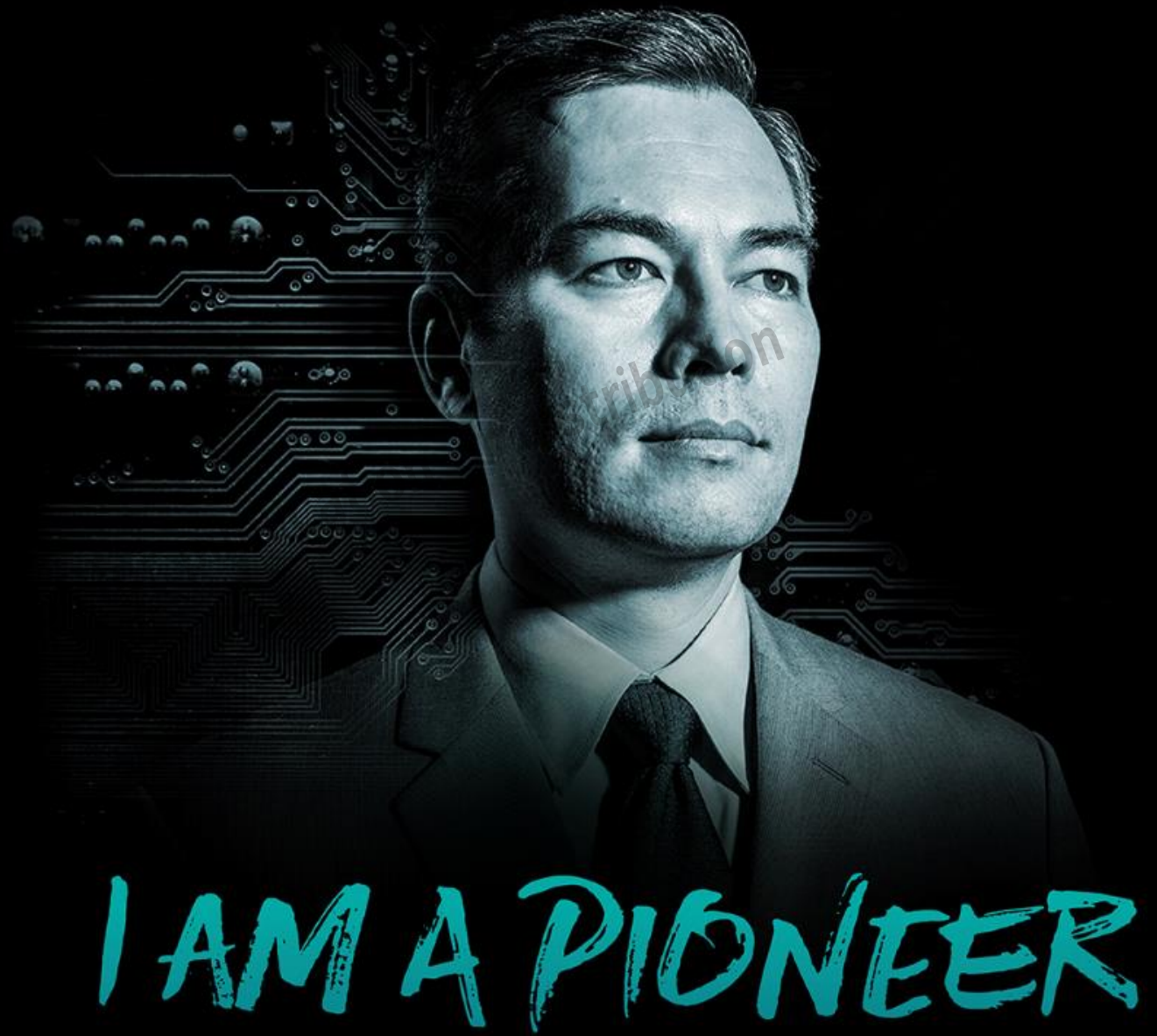
NET2810BE

Feel the vRealize Network Insight

Overcoming Operational Challenges with NSX and Underlay Networking

Andreas Gautschi agautschi@vmware.com
NSX and vRNI Specialist

Karl Fultz kfultz@vmware.com
Solutions Architect



#Vmworld NET2810BE

vmworld 2017

Disclaimer

- This presentation may contain product features that are currently under development.
- This overview of new technology represents no commitment from VMware to deliver these features in any generally available product.
- Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.
- Technical feasibility and market demand will affect final delivery.
- Pricing and packaging for any new technologies or features discussed or presented have not been determined.

Intro

VMware Cloud Management Strategy

Choice of Delivery

Intelligent Operations for SDDC

VMware Cloud Services[1]

Deploy On-premises

- vRealize Automation
- vRealize Business for Cloud
- vRealize Network Insight
- vRealize Operations
- vRealize Log Insight
- Management Packs

Multi-Cloud Management Platform

Delivered as a Service

- Discovery
- Cost Insight
- Secure Networking
- Network Insight
- Wavefront
- AppDefense

Cloud Operations Services:
Management, Governance and Security

vmware ON PREMISES DATA CENTER and CLOUD

Microsoft Azure

amazon web services

Google Cloud Platform

1 – Includes other products or services not listed here

VMware Network Insight: Simplify Cloud Network and Security Operations

Purpose-built for Network Virtualization and Public Clouds

Plan and manage application security

- Understand application dependencies by analyzing traffic flow patterns between VMs
- Accelerate micro-segmentation planning and use firewall rule recommendations to improve cloud security
- Continuously monitor, troubleshoot, and secure clouds

Troubleshoot networks with 360-degree visibility

- Discover and monitor applications across your datacenter and AWS
- Troubleshoot network connectivity issues between VMs with visibility into virtual and physical data center network layers
- Rapidly identify issues through pro-active events and alerts

Ensure health and availability of VMware NSX deployments

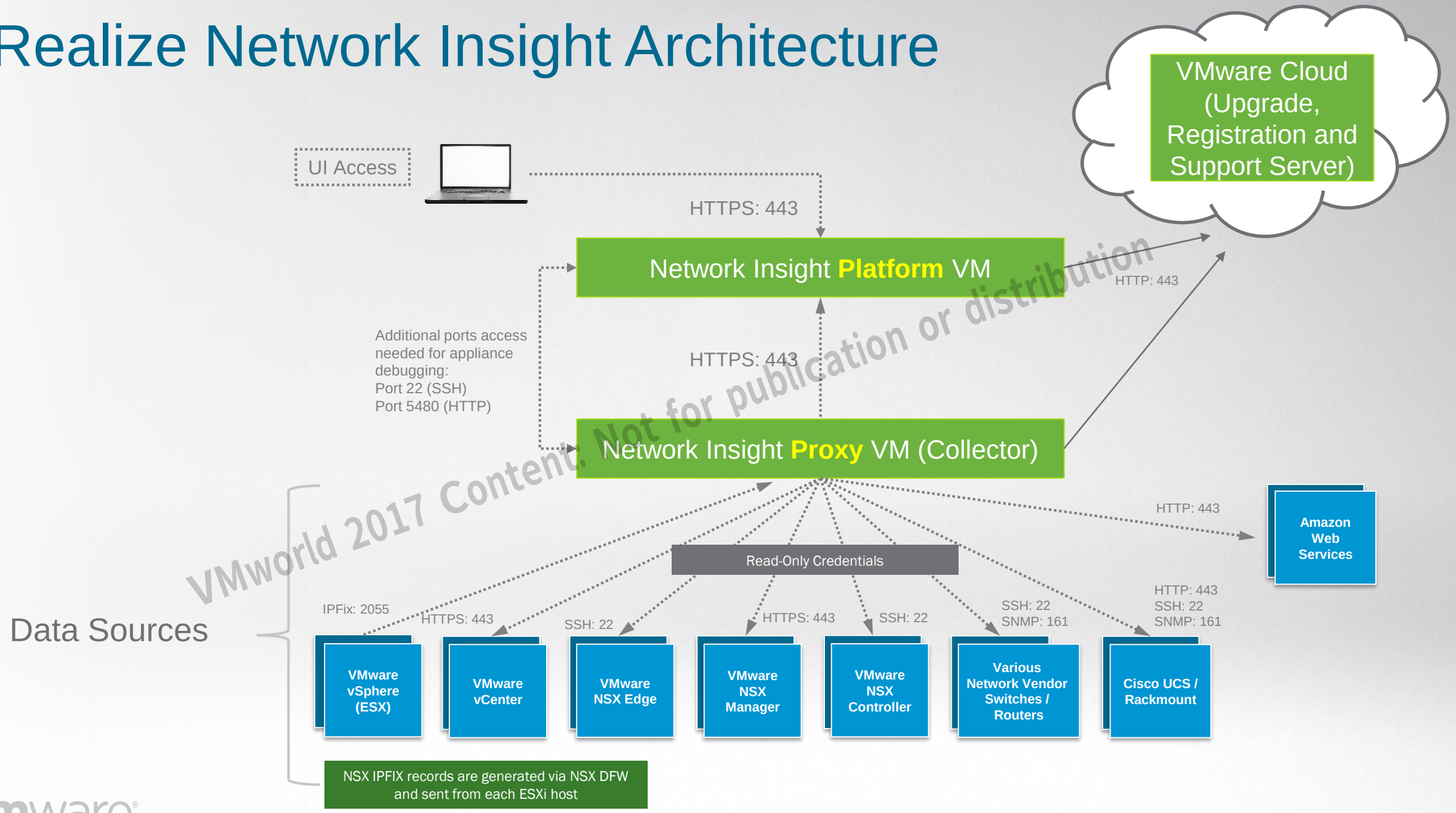
- Scale across large NSX deployments with powerful visualizations for topology and health
- Avoid configuration issues with NSX deployments based on health checklists
- Quickly pinpoint issues for resolution with the help of intuitive UI and search

vmware

Network Insight Feature Comparison

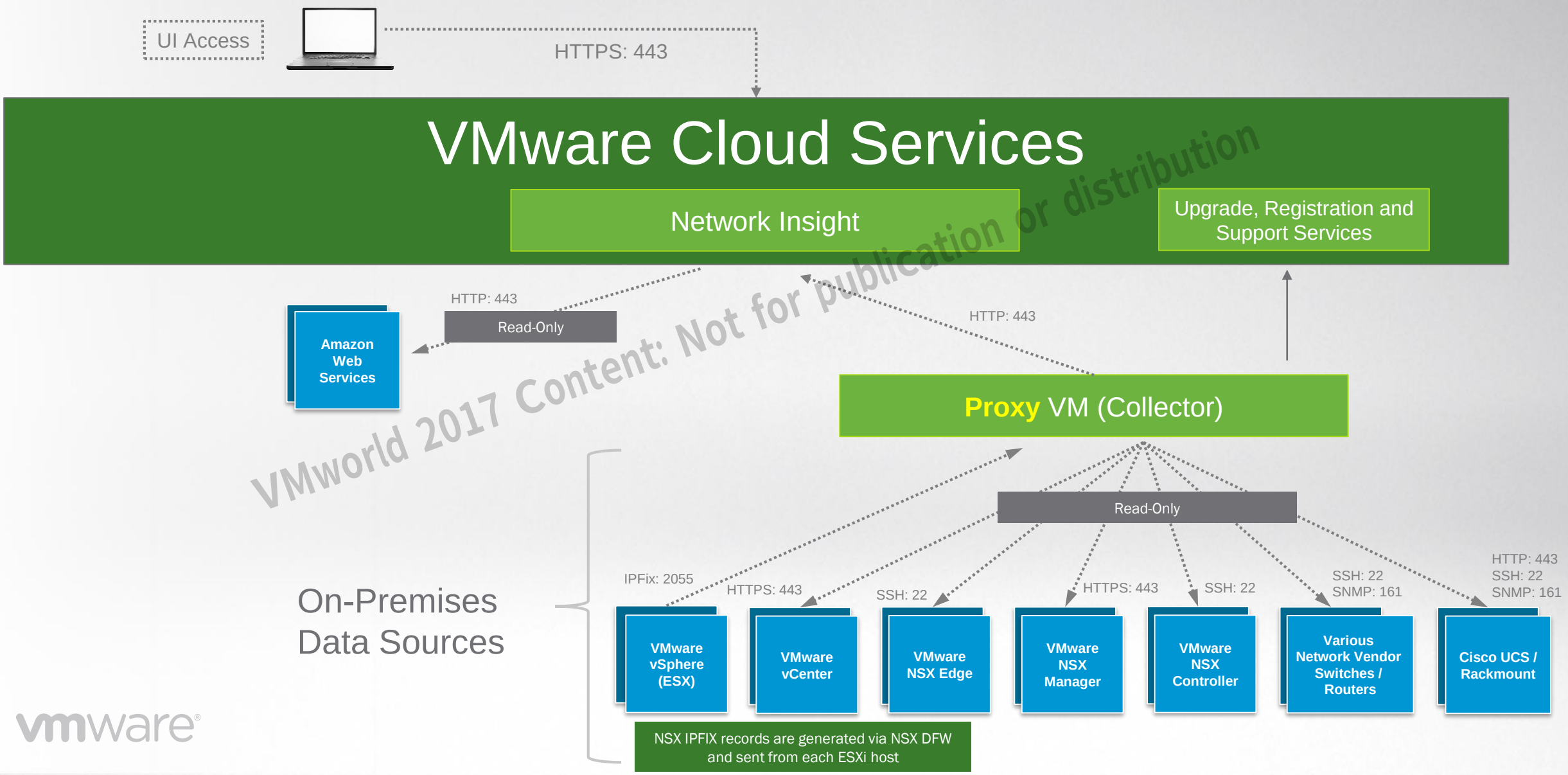
Capability	vRNI ADV	vRNI Enterprise / Network Insight Service
Flow Analysis (VDS IPFIX, V-to-V, V-to-P)	✓	✓
NSX Firewall M-Seg Planning & Operations (NSX IPFIX)	✓	✓
NSX Day 2 Ops (Topology view, best practice checklist, NSX Edge Health dashboard)	✓	✓
VM Paths w/ Physical Switches & Routers	✓	✓
3rd Party Firewall Visibility	✓	✓
AWS VPC, Security Groups, Tags in M-Seg Planning		✓
Visibility and troubleshooting with AWS VPC, EC2, tags, Security Groups		✓
PCI Compliance Dashboard		✓
Configurable and extended retention period for data		✓

vRealize Network Insight Architecture



vmware

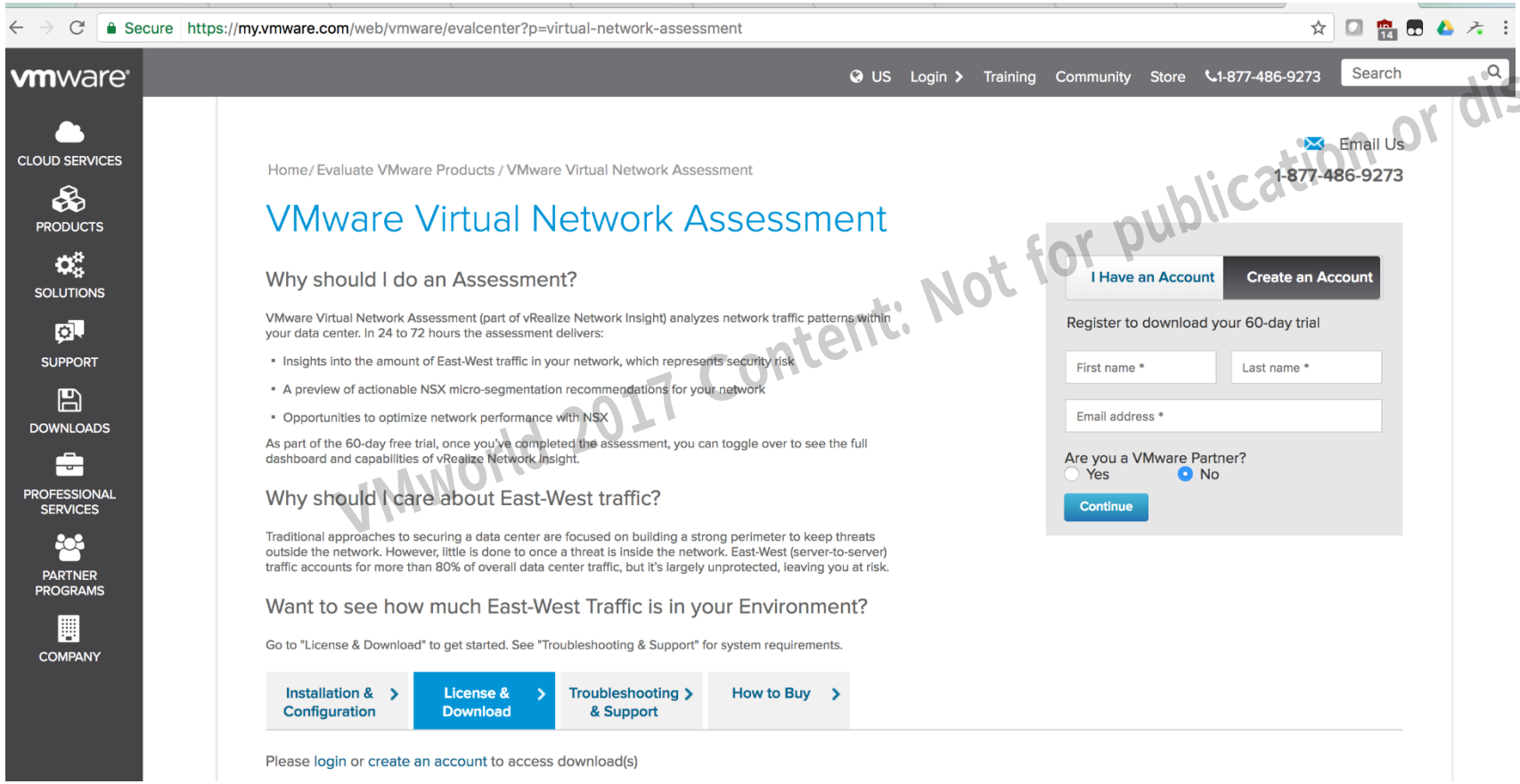
Network Insight Service Architecture



vmware

Our goal today

https://my.vmware.com/web/vmware/evalcenter?p=virtual-network-assessment



Operational Reality

- Usually starts with a phonecall "*You did something and now xyz doesn't work anymore*"
  - "Yes we have noticed this too and are already working on resolving it"
  - "Thanks for letting us know, we are looking into it"
  - "It's not us, maybe try the {insert_tech_silo_here}-guys"
- You typically start with the ops knowledgebase, but if it's a new issue
  - Where do you start
  - Is it infra or app
  - What has changed when, where, why and what
- When you build a private cloud there is no tech silo
- Functions are converging on the hypervisor
- Data spans all over the infrastructure and so troubleshooting spans all over the infra
- "xyz" is usually a multi tiered and distributed system

The troubleshooting process

- Identify a behaviour
- Recreate a behaviour
- Look for potential causes of the behaviour
- Test your theory

Different UIs

Different CLIs

Different languages

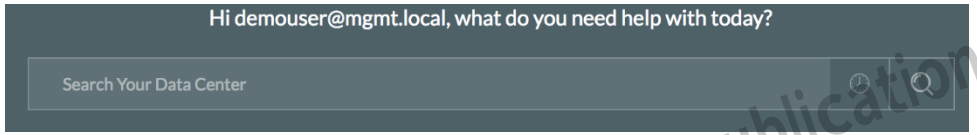
Different concepts

Workload	Ip addr netstat ping traceroute tcpdump
vCenter	Vmotion mac address vnic dvpg flow monitoring traceflow pnics FW rules
ESX CLI	Processes modules vibs logs cdp drops pkt-cap
NSX MGR CLI	Control plane edges dlrs routing tables protocols interface metrics FW rules
Switch CLI	Cdp/lldp interfaces metrics drops ACLs MTU VLAN etherchannel
Router CLI	Cdp/lldp interfaces metrics drops routing procotols tables ACLs def gateways
Chassis UI	Pinning etherchannels vmnics cdp/lldp MTU ACLs VLANs
FW UI/CLI	VLANs def gateways FW rules drops interface metrics cdp/lldp
Log Insight	FW pass/drop/rejects logs from infra and apps
Monitors	Eg. Ping probes db monitors scripts and so on
Others	Eg. Netcool, Netbrain, Solarwinds NPM, CA UIM etc

Enter vRNI

One language: your own

Results in UI



Flow Analysis

Configuration

Metrics

Overlay and Underlay Networks (L2, L3)

FW Rules

Correlation (what when where what else)

Elastic Search

Converged visibility

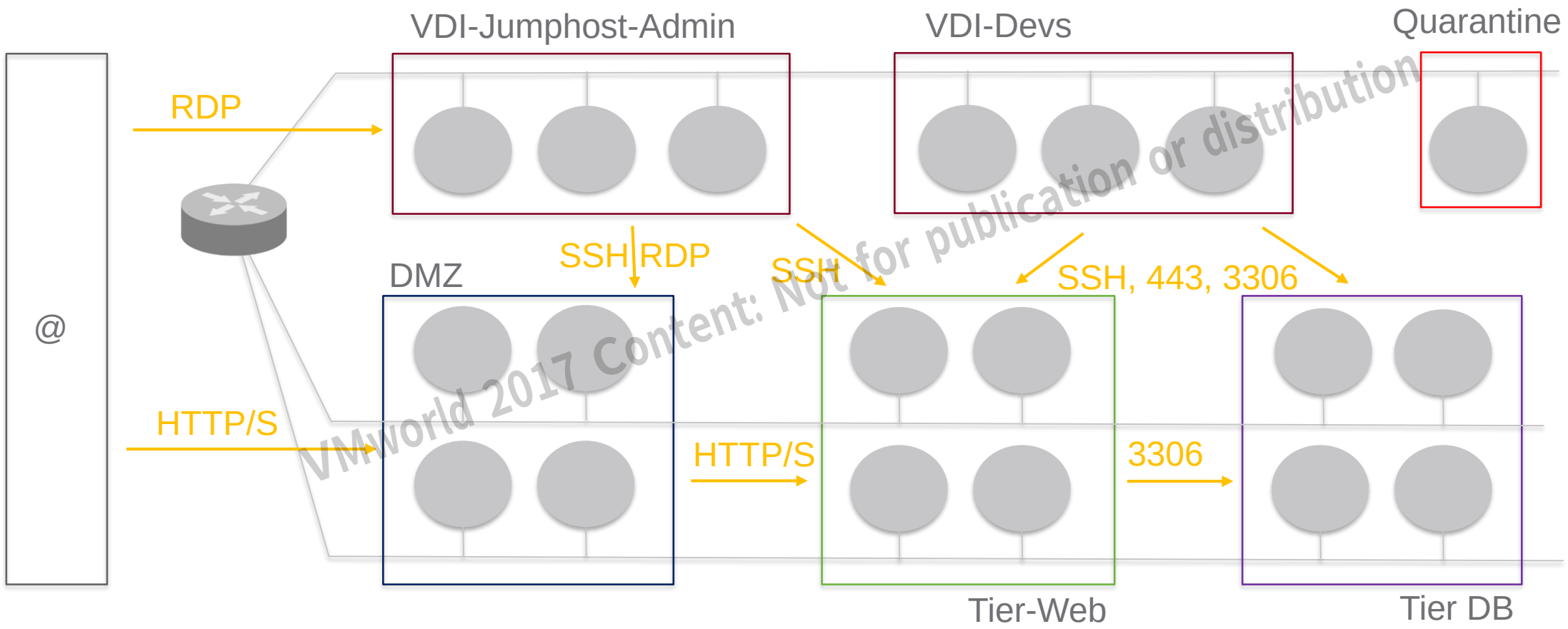
vRealize Network Insight

- vCenter
- ESX CLI
- NSX MGR CLI
- Switch CLI
- Router CLI
- Chassis UI
- FW UI/CLI
- Log Insight

Some sample views

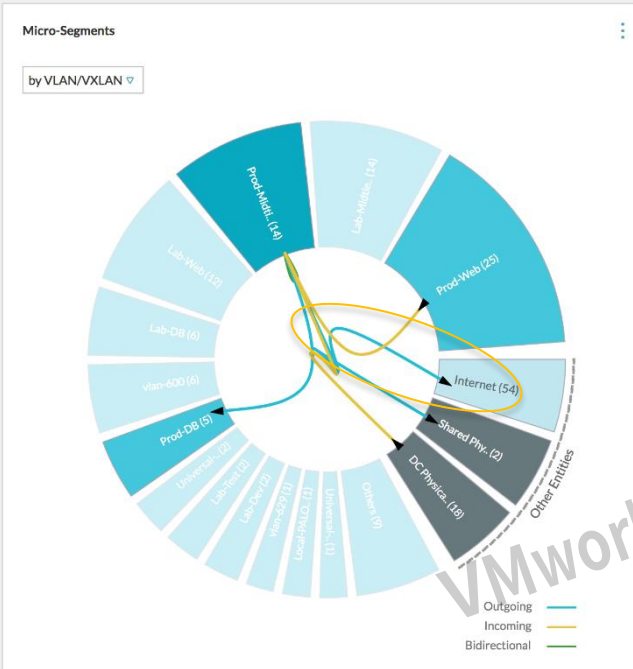
Seeing your infra like you have never seen it before

Sweet spot security planning for NSX



DEMO TIME

- Customer found VDIs being exposed to the internet when they should have been zoned off



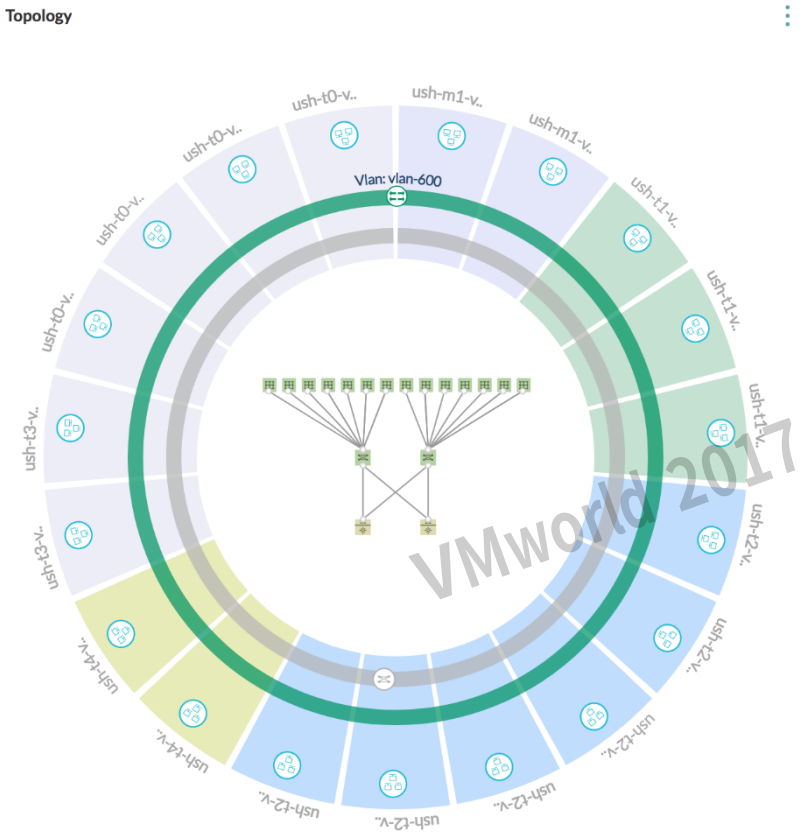
Services in this group	External Services Accessed	Recommended Firewall Rules
42	21	7

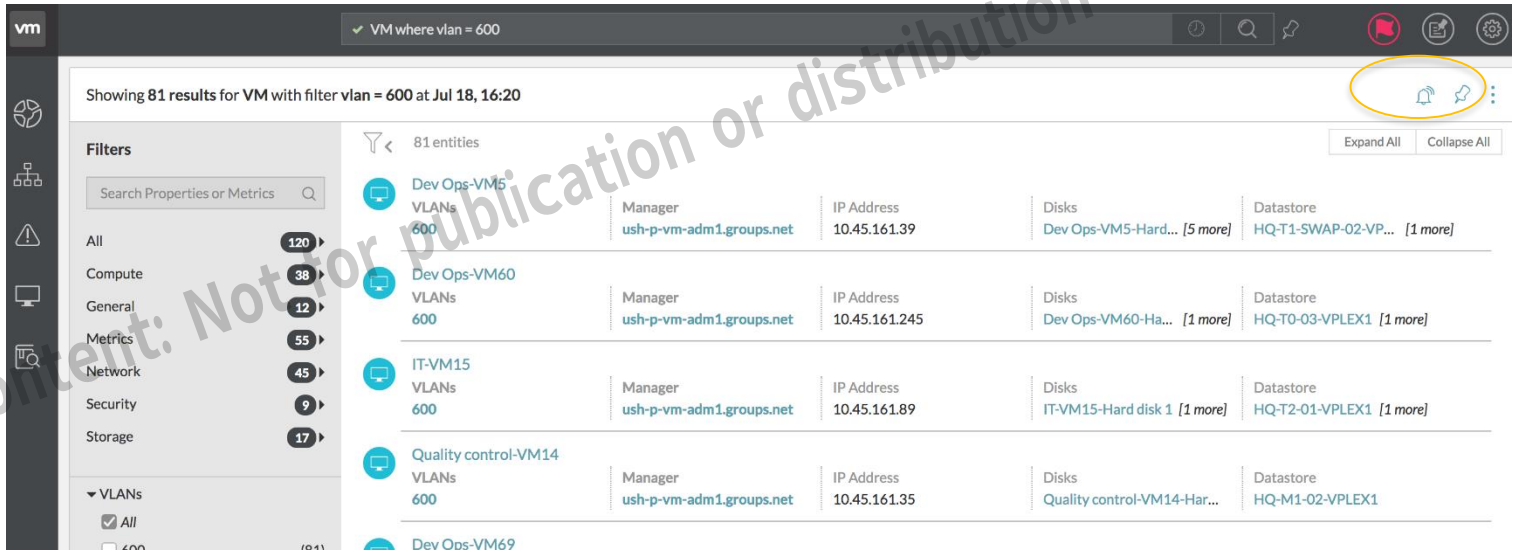
Recommended Firewall Rules

SOURCE	DESTINATION	SERVICES	PROTOCOLS	ACTION
Others_DC Physical	Prod-Midtier	22 [ssh]	TCP	ALLOW
Prod-Midtier	Prod-DB	1521	TCP	ALLOW
Prod-Midtier	Others_DC Physical	389 [ldap]	UDP	ALLOW
Prod-Midtier	Prod-Midtier	9443	TCP	ALLOW
Prod-Midtier	Others_DC Physical	53 [dns]	TCP	ALLOW
Prod-Web	Prod-Midtier	8080	TCP	ALLOW
Prod-Midtier	Others_Internet	443 [https]	TCP	ALLOW

DEMO TIME

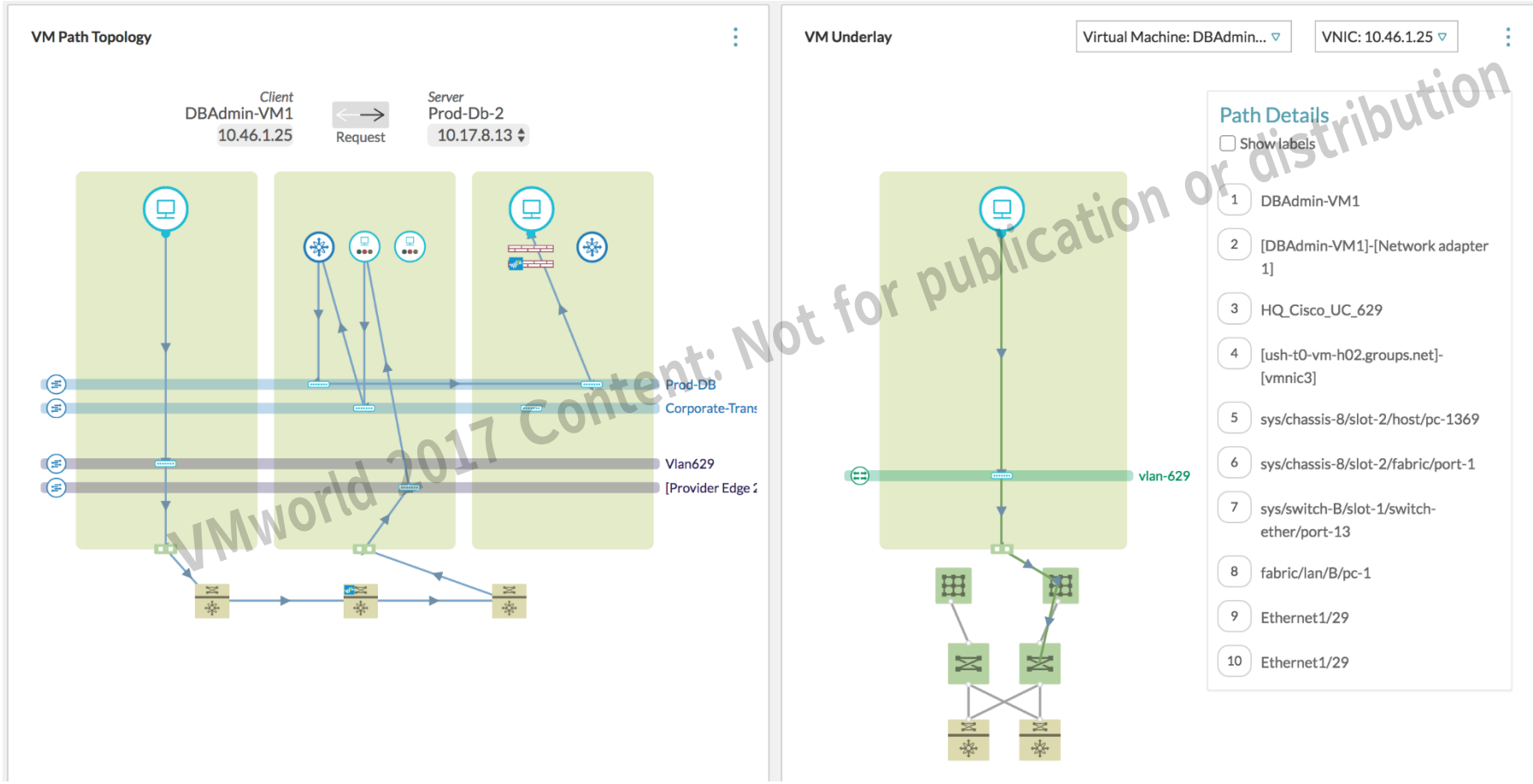
- Customer found production VM on the management network





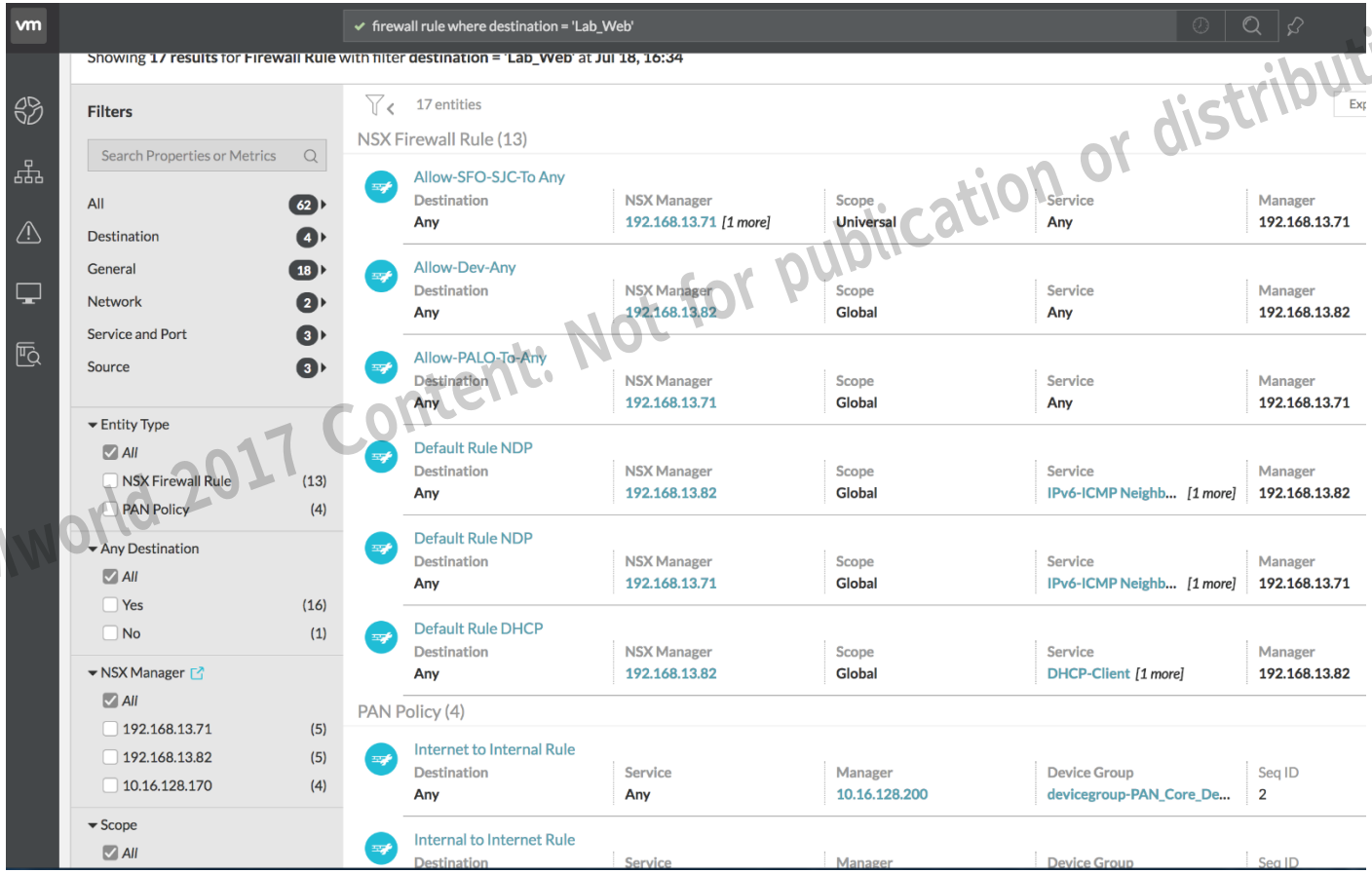
DEMO TIME

- Ended up showing packet walk using vRNI instead of whiteboard



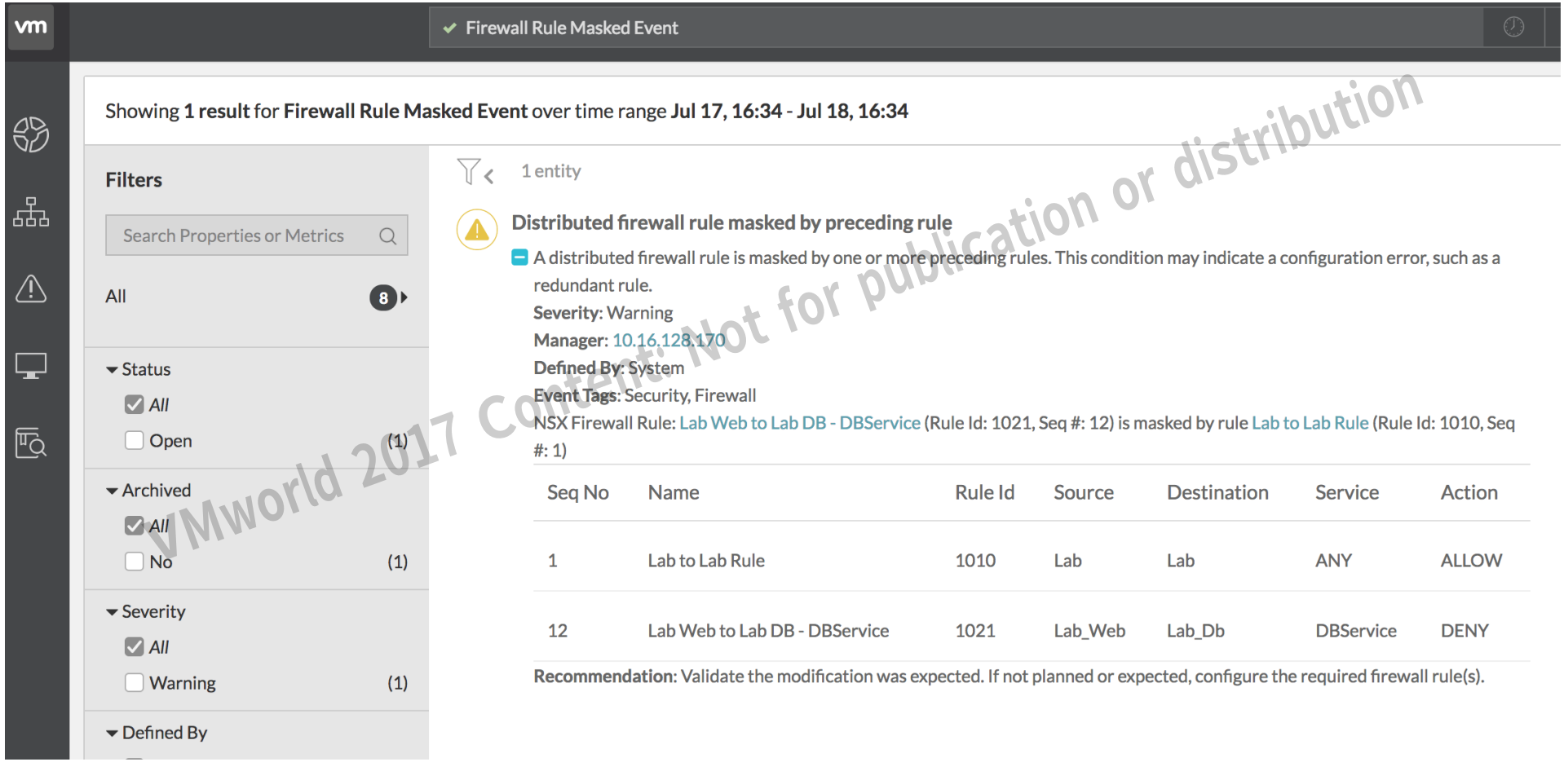
DEMO TIME

- This shows how you can get a view of your FW ruleset across physical, virtual and integrated virtual



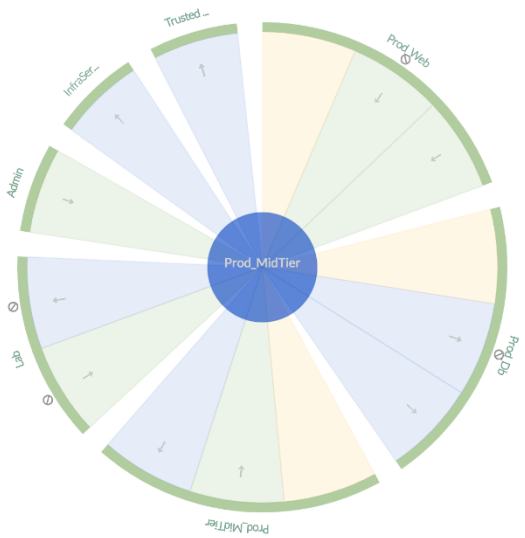
DEMO TIME

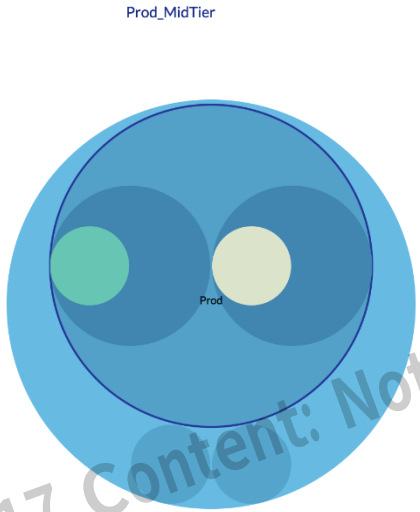
- You can use vRNI to find FW rules that mask each other

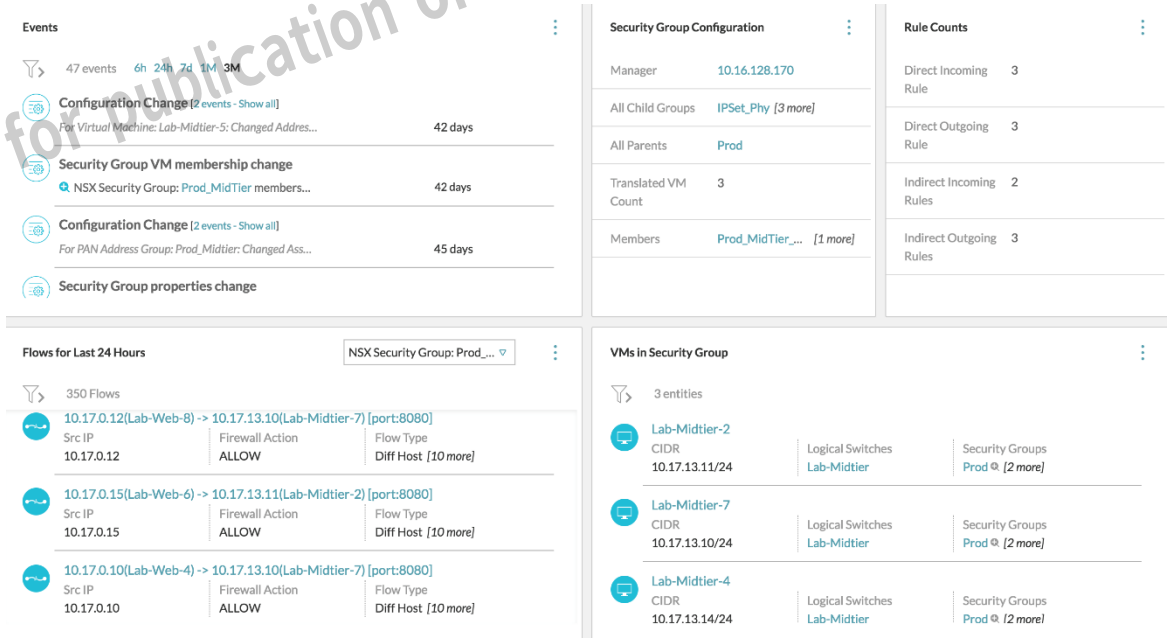


DEMO TIME

- Need to add a demo placeholder slide for the security group view where I show rule inheritance





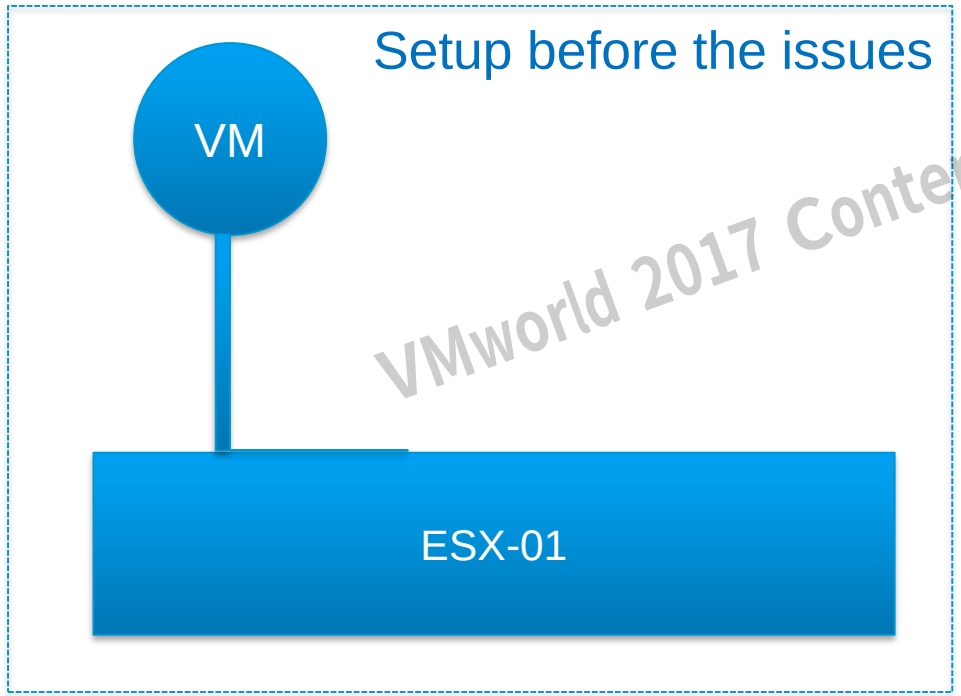


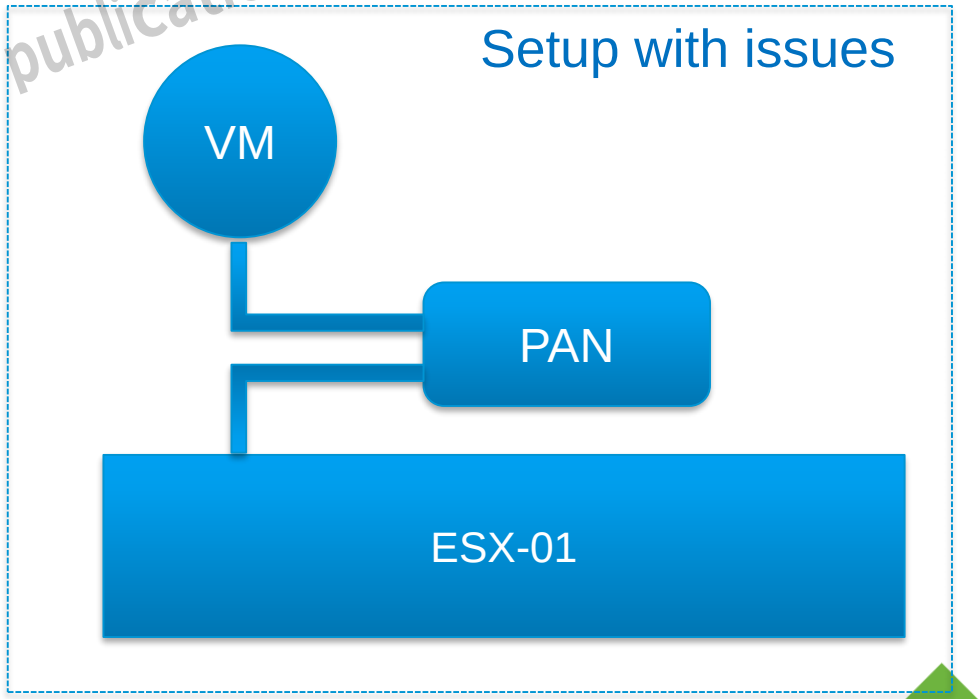
Story time

Useful queries in a real situation

DEMO TIME: Real world troubleshooting – a story

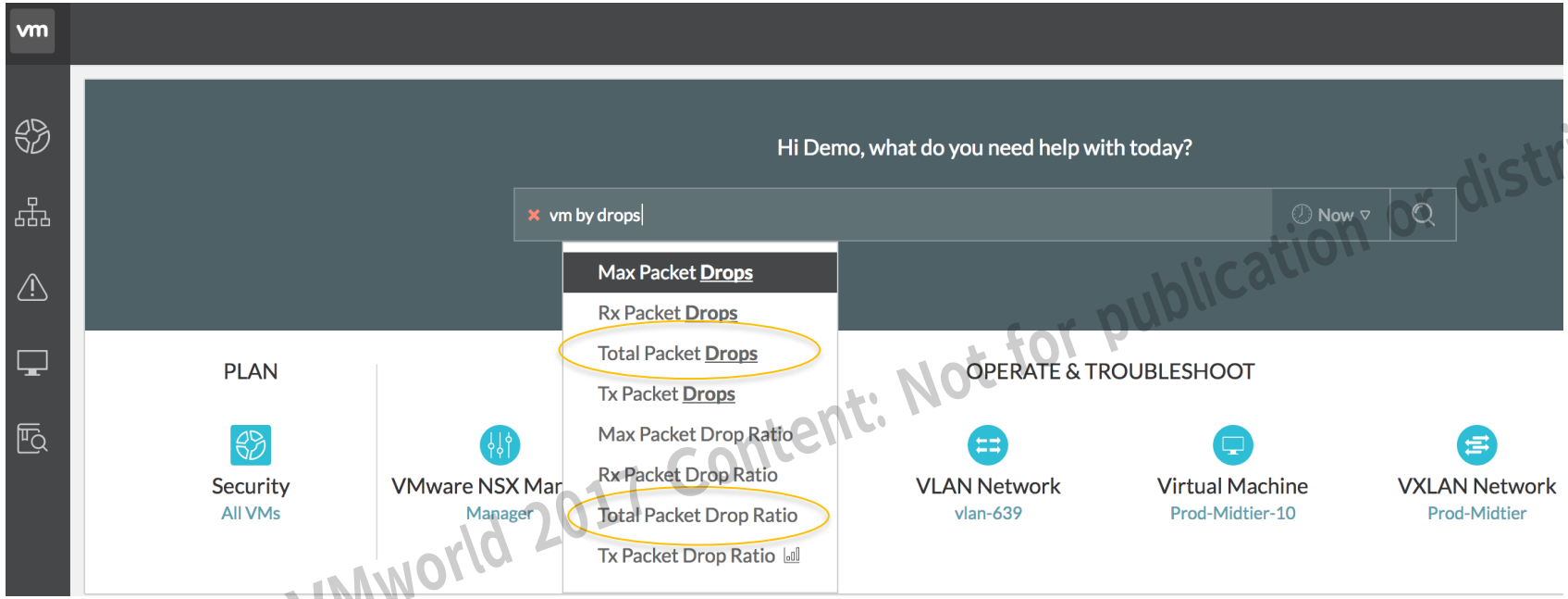
- Customer got a phone call – whenever the DFW with PAN integration was sitting in the datapath, some apps (directory server and MDM system) became very slow, users complained about very long log on times.
- A look on the ping monitors confirmed that the delays went up from <1ms to >50ms on one system, but after vMotion to another system it only went up to to >10ms.





DEMO SLIDE: THIS WILL BE SHOWN ON MBU-LABS OR VIA VIDEO

- Disclaimer: demo shows shows the steps not the actual setup.

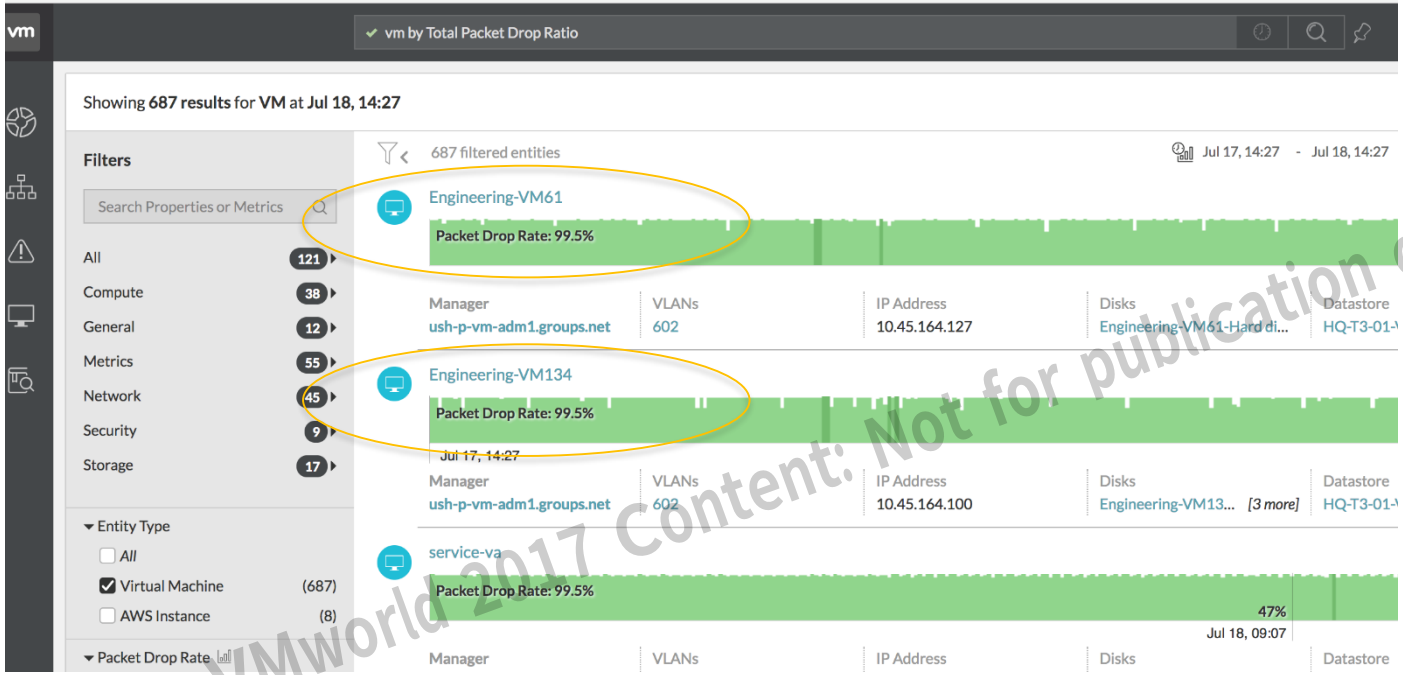


Q To audience: Which metric do you think is better?

A: Packet drop ratio. But the beauty is I don't have to know that, I can try both, or even another, Probably RX ratio would be good enough. The only thing I have to worry about is expressing my idea, search will take care of me and show me whats right. A few years from now you will have a chatbot talking to you and supporting you. Or smth like Siri.

DEMO SLIDE: THIS WILL BE SHOWN ON MBU-LABS OR VIA VIDEO

- Disclaimer: demo shows shows the steps not the actual setup.

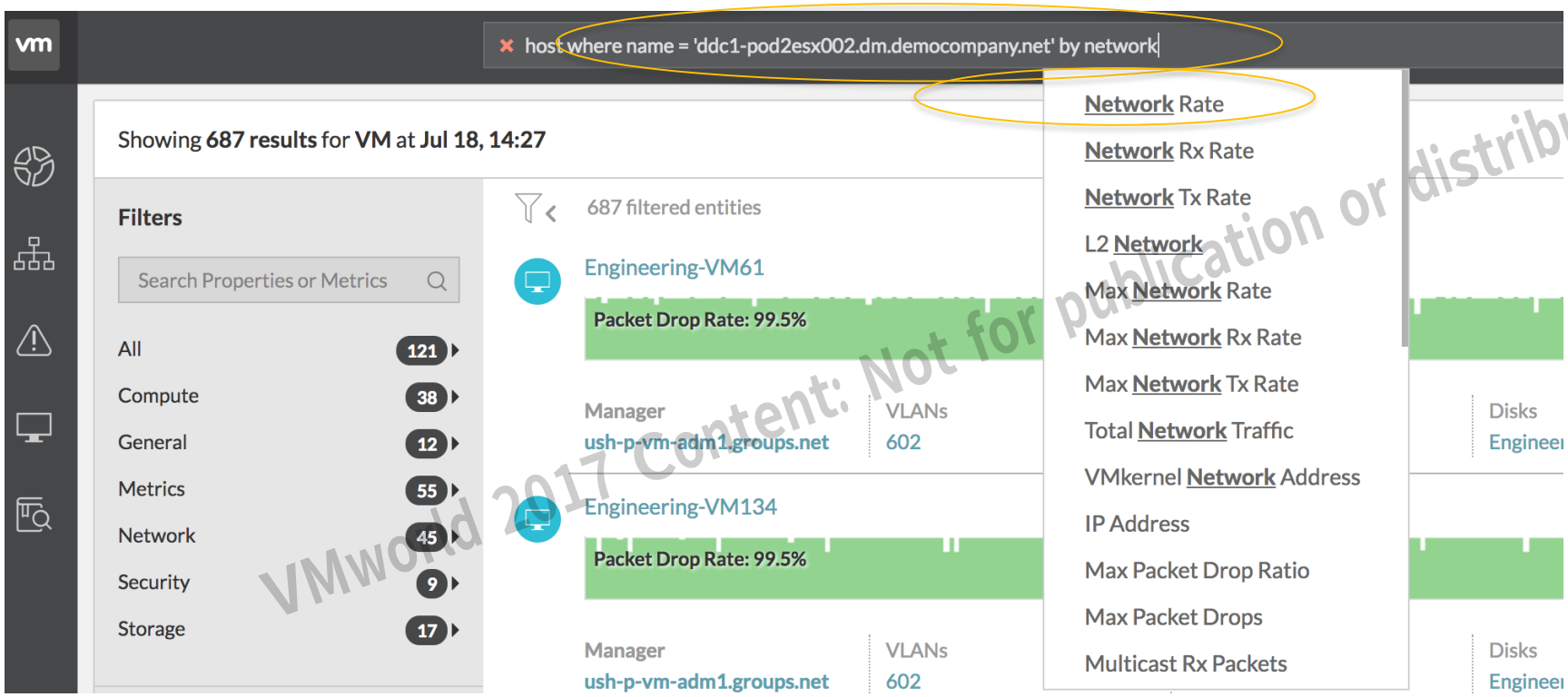


In our case the top droppers were….. The directory server and the MDM VM... The exact VMs that caused the app owners to call.

The idea of checking for packet drops was actually given to me by a partner engineer a few weeks earlier when we discussed virtualisation and he mentioned that he had in many cases been able to find packet drops as a cause of badly performing MS servers.

DEMO SLIDE: THIS WILL BE SHOWN ON MBU-LABS OR VIA VIDEO

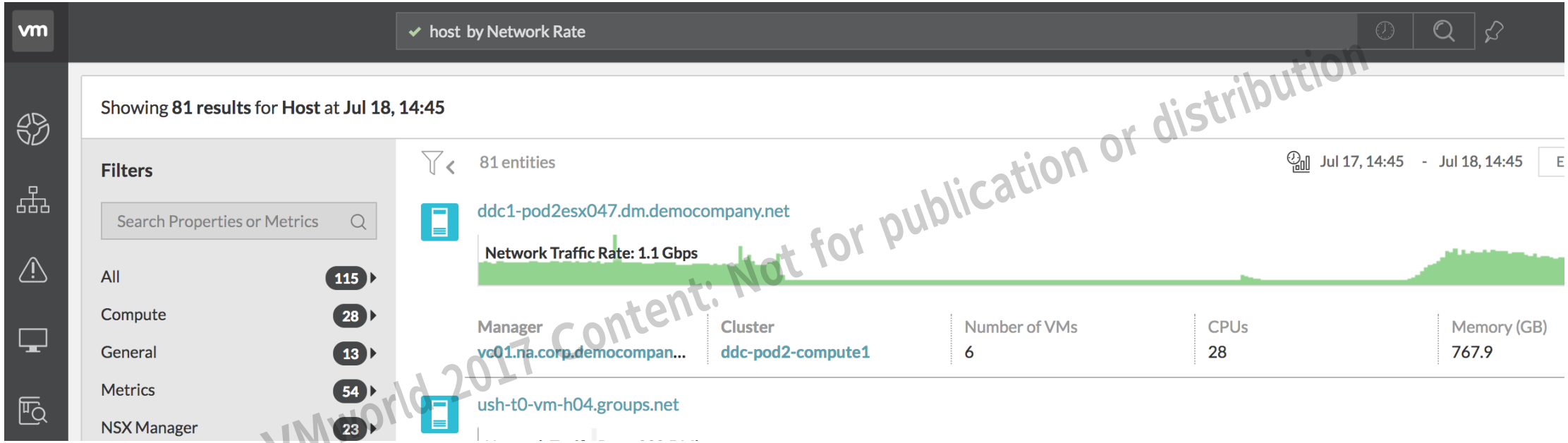
- Disclaimer: demo shows shows the steps not the actual setup.



Again, I don't need to know the actual syntax of what I am doing, all I have to do is express my idea in english. I could have gone for network, for rate or for byte, they all yield the same result.

DEMO SLIDE: THIS WILL BE SHOWN ON MBU-LABS OR VIA VIDEO

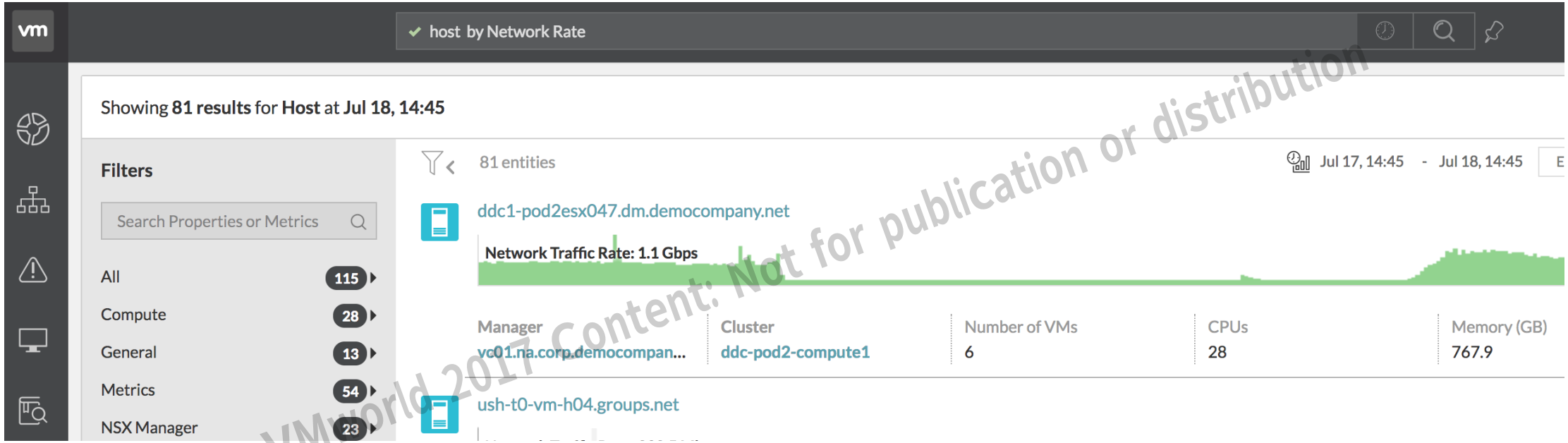
- Disclaimer: demo shows shows the steps not the actual setup.



We knew that all traffic was being sent to the Palo VM and we knew that it shouldn‘t exceed 600Mbps, in our case we saw >750Mbps.... It looked like we hit the nail on the head.

DEMO SLIDE: THIS WILL BE SHOWN ON MBU-LABS OR VIA VIDEO

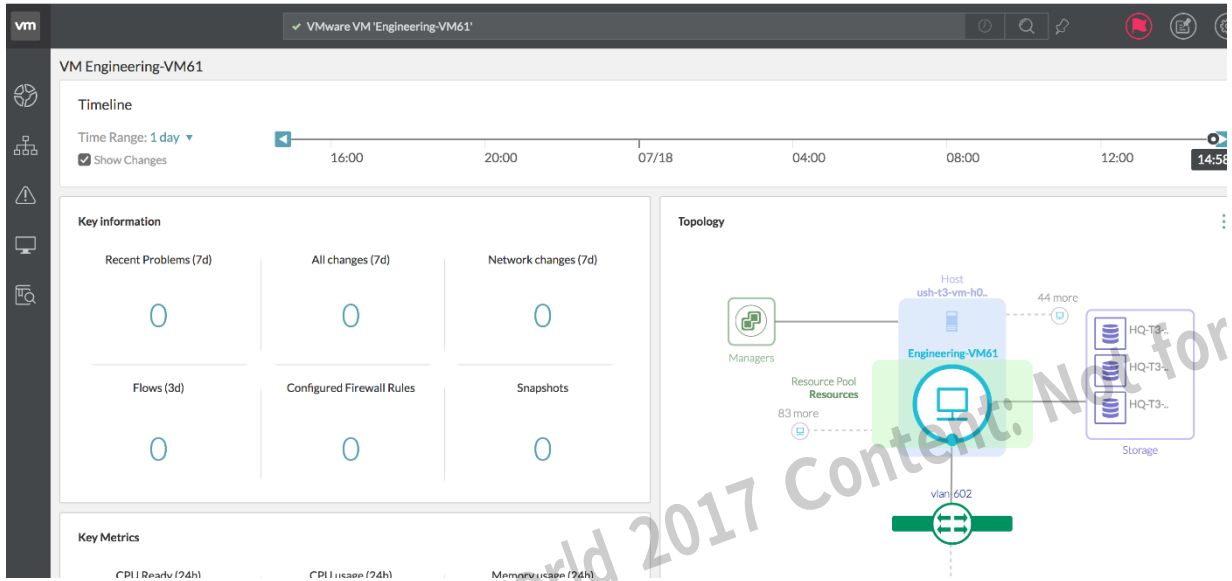
- Disclaimer: demo shows shows the steps not the actual setup.

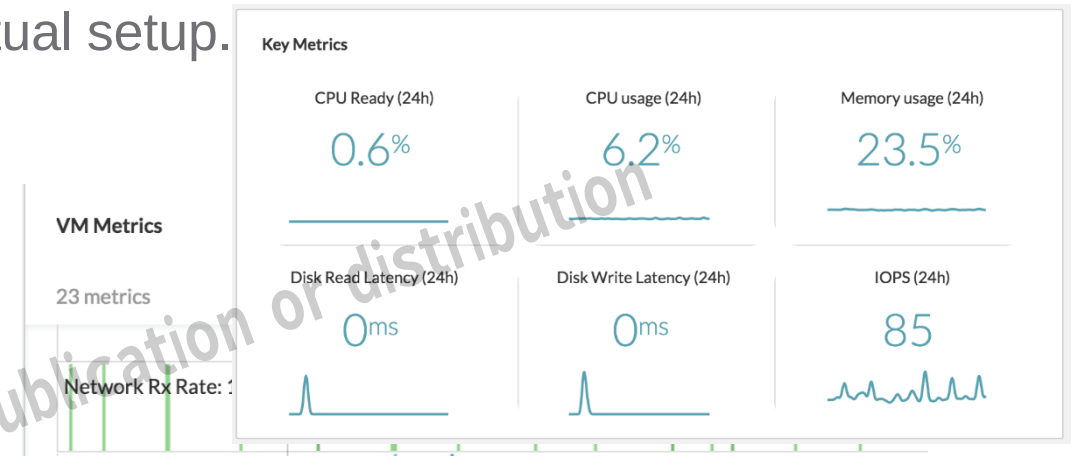


We knew that all traffic was being sent to the Palo VM and we knew that it shouldn‘t exceed 600Mbps, in our case we saw >750Mbps.... It looked like we hit the nail on the head.

DEMO SLIDE: THIS WILL BE SHOWN ON MBU-LABS OR VIA VIDEO

- Disclaimer: demo shows shows the steps not the actual setup.

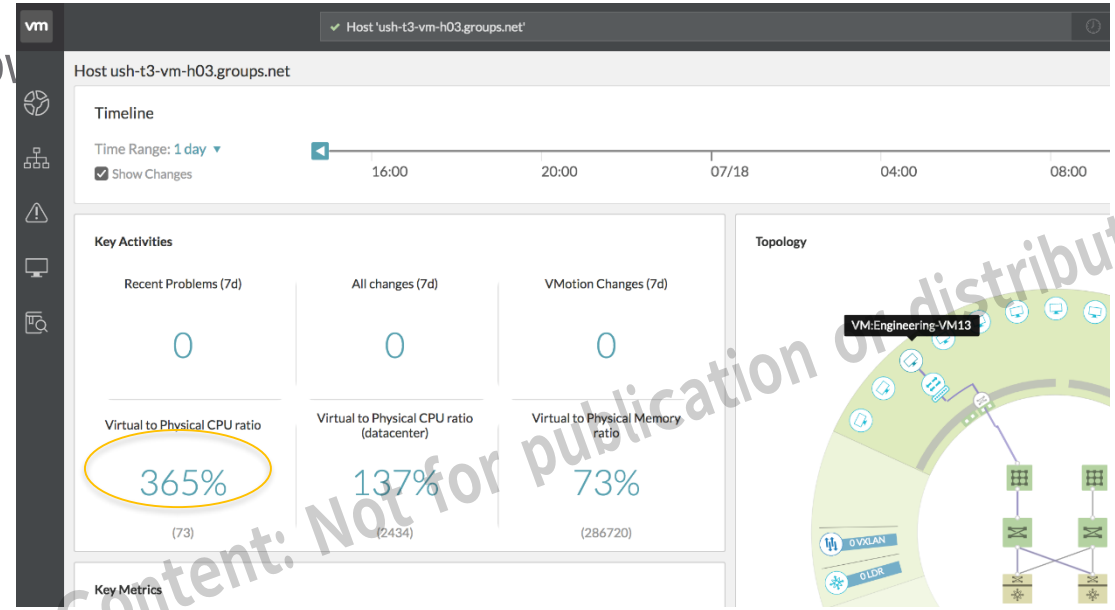




We looked at the VM, we saw the drops in the metrics dash, we saw that the VM was being hosted on host xyz, we saw an elevated CPU ready which indicates that a VM doesn‘t get enough cycles.

DEMO SLIDE: THIS WILL BE SHOWN ON MBU-LABS OR VIA VIDEO

- Disclaimer: demo shows sho



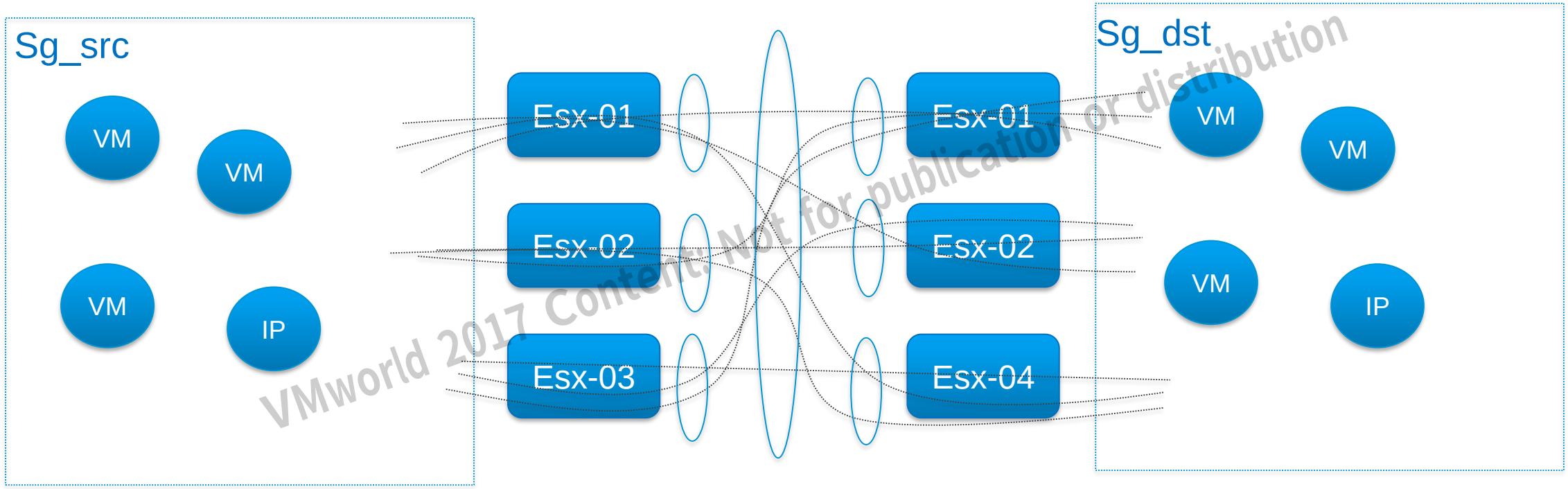
We went ahead and looked at host xyz and found that it was dramatically over subscribed. In our case the host was oversubscribed by >750%.

We do have design guides that allow for oversubscription of up to 800%, DELL best practices recommend to stay under 300%.

In the end of the day it‘s not exact science, it‘s heuristic, it depends on the workload, different workloads react differently, we learned that a directory server is sensitive, so was the MDM VM, other VMs were insensitive, it depends on the application.

How much traffic am I sending to network introspection

Sum (byte rate) of flow where src sg = sg_src and dst sg = sg_dst



… group by src host

… group by dst host

Questions

Please fill out your survey.

Take a survey and enter a draw
for a VMware company store gift card.

vmworld® 2017

vmware®

Tons more – Q&A

- If you have ideas or examples for queries send me an email

Thank You

vmworld®
2017

vmware®