JUNE 2017

vRealize Network Insight

Solution Brief

VMware vRealize® Network Insight™ delivers intelligent operations for software-defined networking and security. It helps customers build an optimized, highly-available and secure network infrastructure across multi-cloud environments. It accelerates micro-segmentation planning and deployment, enables visibility across virtual and physical networks and provides operational views to manage and scale VMware NSX deployments.

This document is a step-by-step guide focused upon key capabilities and the benefits gained throughout a typical 1-2 week deployment.

Data Sheet

Test Drive

Video

vmware®

KEY BENEFITS

- Accelerate micro segmentation planning and deployment
- Audit changes to the security posture and ensure compliance
- Troubleshoot quickly across virtual and physical network and security infrastructure
- Manage and scale NSX deployments with confidence
- Manage network and security across private and public clouds consistently

Solving the Virtual + Physical Network Puzzle

When it comes to managing, troubleshooting, and securing the network, many network administrators face a puzzling, and frustrating, visibility gap across the virtual and physical network. vRealize Network Insight helps with:

Micro segmentation Planning, Deployment and Compliance

- Plan and measure security impact with micro segmentation
- Accelerate micro segmentation deployment with firewall rules recommendations
- Continuously monitor and audit compliance postures over time

360 Network Visibility and Troubleshooting

- Quickly troubleshoot connectivity issues between VMs through powerful path visualization
- Rapidly identify issues through efficient event and alert management
- Unify troubleshooting experience across the virtual and physical infrastructure

Manage and Scale NSX Deployments

- Scale across multiple NSX Managers with powerful visualizations for topology and health
- Avoid configuration issues through an in-product best practices checklist
- Pinpoint and triage issues for quick resolution with intuitive UI and natural language search

Secure Public Cloud Infrastructure

- Extend micro-segmentation planning to AWS security groups
- Analyze traffic flows in AWS and get visibility into AWS Virtual Private Cloud
- Troubleshoot firewall issues between VMs in AWS

Watch Use Case Overview Videos:

Micro-segmentation

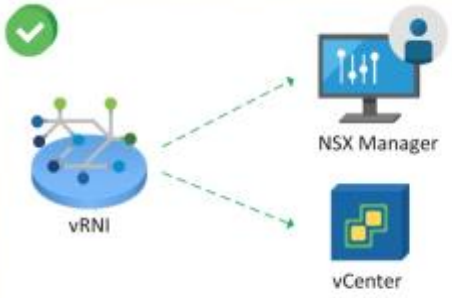
360 Visibility

NSX Operations

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

Phase 1: Enable Infrastructure Components Access and Define Networks

STEP 1



Connect vRNI to vCenter and NSX Manager

KEY BENEFITS

- *Visibility into all vCenter objects and performance metrics*
- *Discover all NSX Security Groups, Firewall Rules, Virtual Networks and NSX Infrastructure Components*

STEP 2

Enable IPFIX (Netflow) on Hosts via vRNI Console

KEY BENEFITS

- *Visibility into all intra and inter host traffic for firewall policy planning (micro-segmentation) and flow monitoring*

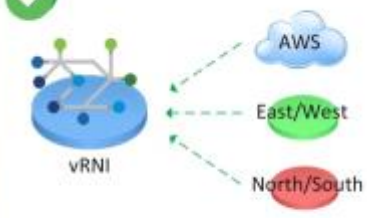
STEP 3

Add Network & Security Data Sources
(Read Only: SSH/SNMP/HTTPS)

KEY BENEFITS

- *Configuration and Performance data collection from physical and virtual network devices for vRNI to stitch together the information for a single, end-to-end view of your Data Center*
- *Support for physical (Firewalls, Switches, Routers, Servers) and virtual (vSphere, NSX Controllers, NSX Edge Gateways and Partner Firewall vendors)*
- *Support for AWS VPC flow logs*

STEP 4



Define Network Segment Ranges

KEY BENEFITS

- *Flexibility to specify datacenter public IPs to be treated as non Internet IPs while tagging flows and micro-segmentation.*
- *Specifying these IP segments provides a more accurate view of true North-South and East-West traffic for security planning and flow visualization*
- *Add-in AWS VPC, security groups and subnets identified through VPC flow logs*

Phase 2: Verify Connectivity and Plan Security

STEP 1

Path Analysis

KEY BENEFITS

- *Test App to App connectivity with easy to use google-like searches to verify all virtual and physical network devices were discovered and are being managed*
- *Provides a dynamic topology map based upon application flow to easily pinpoint networking and security issues*
- *Ability to save any of the searches for customizable alerts*
- *Troubleshoot VM to VM connectivity on AWS through security groups and rules*

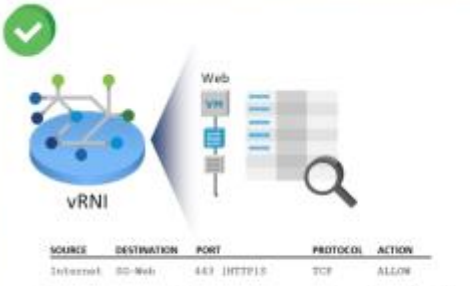
STEP 2

Create Application Groups

KEY BENEFITS

- *Define your own application for easy reference and troubleshooting. vRNI enables users to create a grouping of VMs and devices for their specific needs. For example, users can define an arbitrary name of myCustomApp1 to represent all components of a specific 3 tier application.*
- *Applications can be purely on-premise, public or hybrid*
- *Once created, users can perform custom alerts and/or pin boards that can easily be shared and searched against. If any component of this application grouping has issues, vRNI will be aware and will update the topology map and/or alert as configured.*

STEP 3



Review Recommended Micro-Segmentation Firewall Rules

KEY BENEFITS

- *Since Day 0, vRNI has been analyzing all East-West and North-South flows in the Data Center. As a result, a very precise firewall micro-segmentation white-list policy is developed for review and export to NSX manager*
- *vRNI recommended firewall groups and rules are based upon actual traffic flows observed*
- *AWS Security Group Rules can also be determined using AWS flow data*

Phase 3: Best Practice Check; Data Center Timeline and Alerting

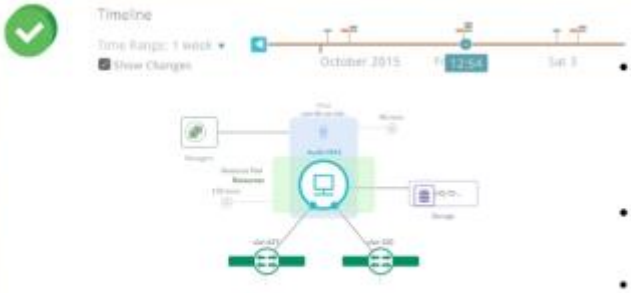
STEP 1

NSX Best Practice Checks

KEY BENEFITS

- *Provides an easy to read summary of NSX related issues and alerts against dozens of VMware's Networking and Security best practices.*
- *Easily remediate identified issues with provided recommendations*
- *Automatically detects configuration errors in mismatch segment ID, IPset definitions, etc.*

STEP 2



Network and Security Data Center Timeline

KEY BENEFITS

- *The Network and Security timeline provides the ability to look at the configured state of the data center at a particular time in the past and a bird's eye view of events that were detected across a selected time range.*
- *From the Time Range option, you can select the time range of the timeline that you want to view (up to 30 days)*
- *A small grey horizontal bar denotes an event and a small red horizontal bar denotes a problem*

STEP 3

Setup Custom Alerting Events and Severity Levels

KEY BENEFITS

- *In addition to pre-defined system level events, User-defined events enables custom alerting capabilities by using any of the vRNI searches as an event type. Users can define specific application, device, security or network alerts based upon their monitoring needs*
- *The event is triggered either when search results change or when no results are returned. If the event is marked as a problem, a severity designation will be associated*
- *Events may also be crated and monitored for AWS entities suchas EC2 instances, VPC, Security Groups, tags, etc...*

STEP 4

Custom Defined Dashboards using Pins

KEY BENEFITS

- *Every pane within vRNI is available to be added to custom pin boards for easy access to Network, Security and Device information.*
- *A pin board can be defined for a specific critical application where a single dash board can provide end-to-end connectivity, device metrics, problem alerts, etc...*
- *Enables Application owners, NOC, SOC users visibility with read-only access via a secure URL.*

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

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