

# AutoNSX

## The best software to build security models

Simple 5 step rule migration from vRNI

Organizations today demand an agile data center environment to reduce IT costs, increase business agility and remain competitive. Security has traditionally been “lost” in the transition. What’s more, traditional security approaches are manual, operationally complex, slow and unable to keep pace with dynamic changes and rapid application provisioning.

Organizations often focus on the tools and processes that cover security area, but it comes with huge operation overhead to support organizations to apply correct rules and securing new or already existing applications. Here AutoNSX and vRNI come together to solve the issue.

***“VMware vRealize Network Insight helps you build an optimized, highly available and secure network infrastructure across hybrid and multi-cloud environments. It provides network visibility and analytics to accelerate micro-segmentation security, minimize risk during application migration, optimize network performance and confidently manage and scale NSX deployments.”***

VMware vRealize Network Insight can give NSX Firewall Rule recommendations-based user defined “applications” via different criteria. All rules are easy to understand by Security personnel. When it come to apply rules then it requires an operational manual migration from wat vRNI propose to the actual useable rule sets. AutoNSX help to solve this issue and allow security to be in place with workflow based 5 step migration.

### Automated Security provisioning

AutoNSX allows create policy-based rules from vRNI to NSX in automated fashion. All rules a migrated as seen in the vRNI per application basis. Security zone, security groups, security tags, IPset’s are created automatically as they are defined in vRNI Application name.



Organizations today spend time and money to perform such tasks. Key metrics, to migrate one application from vRNI or build it from scratch, time required is about 8 hours for one FTE, with AutoNSX rule migration including groups creation, security zone, security groups, membership assignments it is done in 5 minutes. Which reduce time to marked deployments to a minimum level.

# AutoNSX

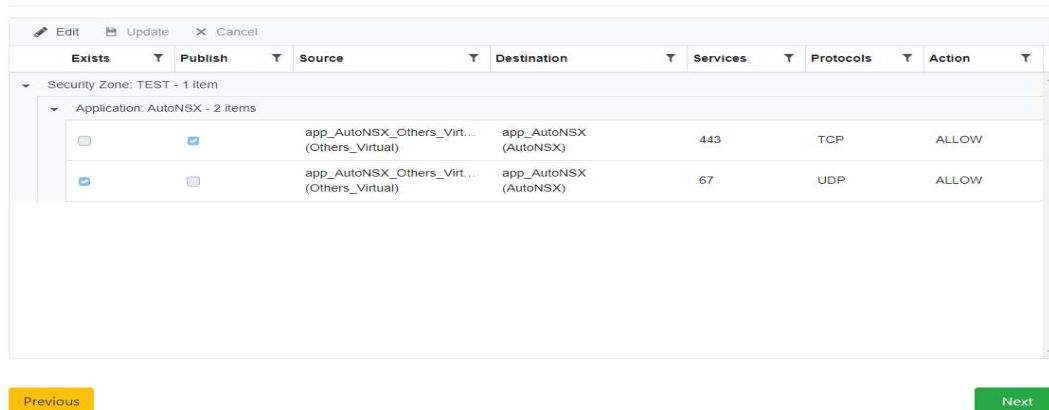
## The best software to build security models

Simple 5 step rule migration from vRNI

### Simple Interface/ Workflow based

Built with World-class interface used with security as a top priority and user-based authentication with encrypted communication. Workflow defined task and migration

Choose the recommended rules that will be published to NSX.



### AutoNSX features:

- Uses existing Security groups in NSX
- Create new Security groups
- Create Security zones
- Create Security Tags
- Create IPset
- Create Security policy (firewall section in NSX-V)
- Check for duplicated rules
- Granular rules publish, selective or all in one
- Shared security groups between applications
- Dynamic member ship assignment
- Update of exiting items in NSX
- Multiple data source within the same platform
- Macro-segmentation (a.k.a Application isolation)
- Micro-segmentation (by tier)

### AutoNSX benefits:

- No manual rule exports
- Accelerates business security
- Reduce time to market deployments
- Eliminate human errors
- Licensed based on data source, not based on CPU count and size of deployments
- Single appliance with minimal hardware resources
- Virtual based appliance
- Reduces CAPEX and OPEX in comparison with others
- Guaranteed privacy
- No rule manipulation or retention in appliance storage
- Act as transparent broker