

**Security Policy Management for the Software-Defined Data Center**

Many organizations are now looking to take advantage of the flexibility and cost savings of the Software-Defined Data Center (SDDC). But taking the first steps towards migrating network security to a SDDC can seem overwhelming. Discovering application connectivity dependencies and creating policies for VMware NSX firewalls that will securely manage micro-segments within the SDDC is extremely challenging. Moreover, VMware NSX firewall policies must be managed in conjunction with the rest of your enterprise security infrastructure in order to ensure that your organization is fully secure and compliant.

**The AlgoSec Security Management Solution**

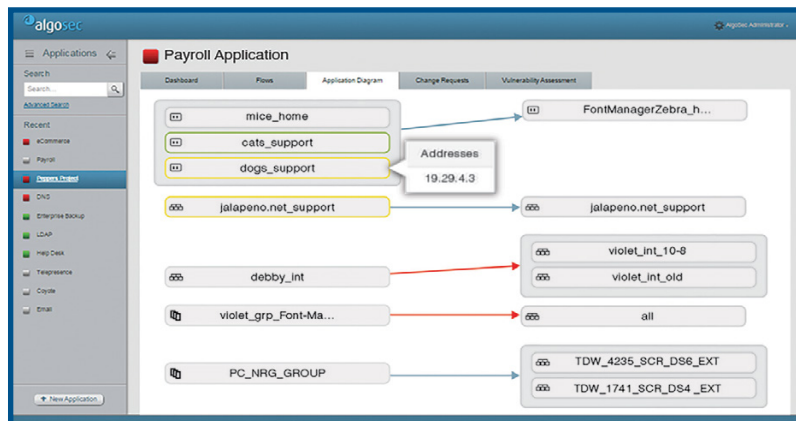
The AlgoSec Security Management Solution integrates with VMware NSX distributed firewalls to deliver unified security policy management across your traditional on-premise data center and your SDDC. AlgoSec supports the entire security policy management lifecycle — from application connectivity discovery and migration, through ongoing management and compliance, to secure decommissioning.

**Discover & Map**

AlgoSec automatically identifies all applications and their connectivity flows across your data center, and generates an up-to-date map of your environment — without requiring any prior knowledge or manual configuration by security, networking or application experts.

**AlgoSec Security Management Solution for VMware NSX**

- Discover and migrate application connectivity flows to the SDDC
- Easily create VMware NSX security policies for micro-segmentation
- Unify security policy management across your entire enterprise
- Automatically manage all changes to network security policies and eliminate misconfigurations
- Proactively assess risk and ensure continuous compliance
- Get a tighter security that provides better protection against cyber-attacks



## Migrate Connectivity

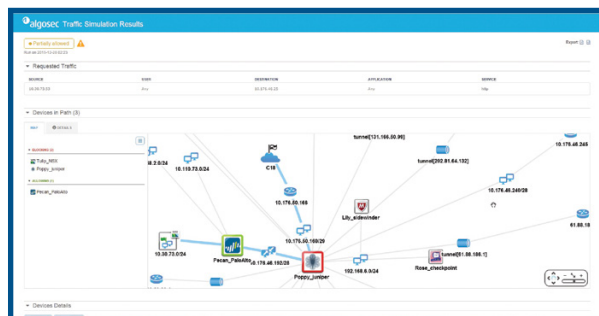
Once identified, AlgoSec can automatically migrate the relevant application connectivity flows to your SDDC — thereby simplifying an extremely complex and risky process, and saving significant time and effort.

## Create Security Policies for Micro-segmentation

Using AlgoSec you can easily create East-West firewall security policies to support your micro-segmentation strategy within the SDDC. Instead of trying to manually figure out all the connectivity flows for each application, you can simply select individual flows or groups of flows from the application connectivity map and assign them to specific micro-segments.

## Visualize

AlgoSec provides full visibility across your entire enterprise environment, including all security devices from any vendor, in a single pane for easy management and troubleshooting of network security policies.



## Support for Heterogeneous Environments

In addition to VMware NSX, AlgoSec seamlessly supports traditional and virtual firewalls, NGFWs and cloud controls as well as routers, load balancers and web proxies from the leading vendors to deliver unified security policy management across heterogeneous environments.

### Supported Cloud Platforms



### Supported Network Security Vendors



#### Global Headquarters

65 Challenger Road, Suite 320  
Ridgefield Park, NJ 07660  
USA  
+1-888-358-3696

#### EMEA Headquarters

80 Coleman Street  
London EC2R 5 BJ  
United Kingdom  
+44-207-099-7545

#### APAC Headquarters

10 Anson Road, #14-06  
International Plaza  
Singapore 079903  
+65-3158-2120

#### AlgoSec.com

