AutoNSX- Segmentation made *Easy*

PARTNER SOLUTION BRIEF: AutoNSX

vmware®

Micro-Segmentation implementation in Software-Defined Data Center

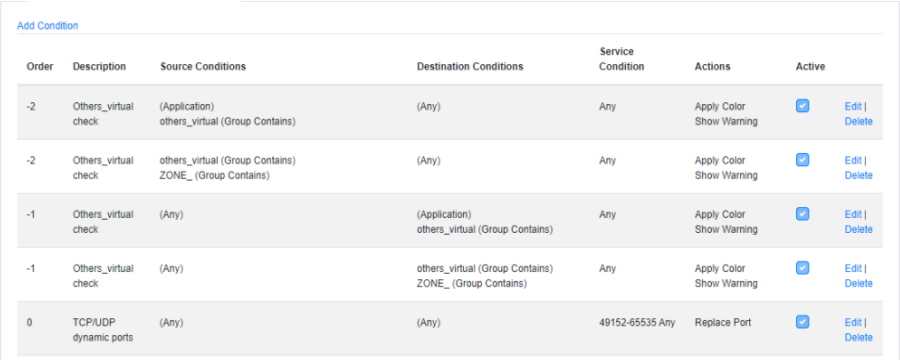
Many organizations are now are in the process of securing their SDDC. The main techniques in this process are called micro-segmentation. However, implementation of micro-segmentation always was one of the most complicated processes, that requires hours spend in design, scripting and implementation. AutoNSX simplifies entire process of micro segmentation.

The AutoNSX Software Solution Integrates with VMware NSX

The AutoNSX Software Solution integrates with VMware NSX distributed firewall and automate segmentation implementation in matters of minutes. AutoNSX supports the entire security policy management of NSX. Entire organization can benefit from AutoNSX Software Solution, as it provides full visibility to Application Owners to the implemented security to their applications. Any organization unit with the organization benefits from AutoNSX from Product Owners to Security Architects and Security Engineers. AutoNSX abstracts complexity of implementation of micro-segmentation by leveraging VMware NSX constructs (Tags, Groups, Polices).

The AutoNSX Software Solution Integrates with VMware vRNI

AutoNSX integrates with VMware vRNI to receive data feed, like Applications, network flows, recommended security rules. Received flows and security rules are enriched and sanitized from duplication. Additionally, Security Team can create Unified Global Security Rules that are applied to any of the segmented applications. AutoNSX gives ability to set up set of conditions against traffic flows and communication patters and display those during the segmentation of an applications. For example: Replace ports with range of ports or prohibit segmentation in case of security zone violation, traffic from Production Zone to Sandbox Zone.



Add Condition

Order	Description	Source Conditions	Destination Conditions	Service Condition	Actions	Active	
-2	Others_virtual check	(Application) others_virtual (Group Contains)	(Any)	Any	Apply Color Show Warning	☑	Edit | Delete
-2	Others_virtual check	others_virtual (Group Contains) ZONE_ (Group Contains)	(Any)	Any	Apply Color Show Warning	☑	Edit | Delete
-1	Others_virtual check	(Any)	(Application) others_virtual (Group Contains)	Any	Apply Color Show Warning	☑	Edit | Delete
-1	Others_virtual check	(Any)	others_virtual (Group Contains) ZONE_ (Group Contains)	Any	Apply Color Show Warning	☑	Edit | Delete
0	TCP/UDP dynamic ports	(Any)	(Any)	49152-65535 Any	Replace Port	☑	Edit | Delete

AutoNSX Solution for VMware NSX

- Discover and migrate security rules from VRNI to VMware NSX
- Easily create manage and update VMware NSX security policies for the micro- segmented environment
- Unified Global Security Rules Automatically
- Integration with Service Now CMDB to ensure governance and change management
- Prohibit "blindfold" implementation of well know malicious IP addresses during micro-segmentation
- Application Owners full visibility to security policies applied to their applications
- "Four eyes principle" approve any action before it can be executed

vmware® PARTNER TECHNOLOGY ALLIANCE

The AutoNSX Software Solution Integrates with Service Now & CMDB – “four eyes principle”

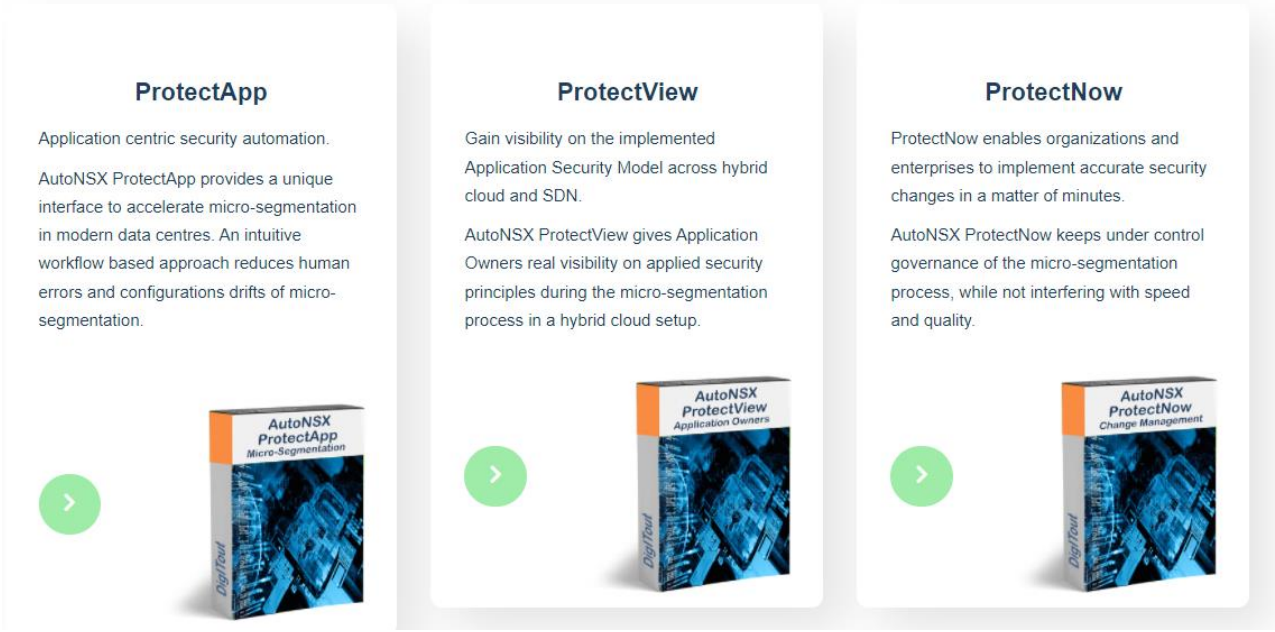
AutoNSX integrates with Service NOW CMDB and updates application CI with security rules and objects created in VMware NSX. Any changes triggered in CMDB reflects on security policies. Application Owners can define their applications in Service Now and AutoNSX will automatically takes care of the Application Security. Entire process can be adjusted to be fully autonomous, partly manual for only manual. This ensures that any organization can tweak AutoNSX to match the company’s workflow process. The AutoNSX integration engine updates VMware vRNI Application members in case of any changes in CMDB which reduces TCO on running the latest licensing on entire software stack.

“**Four eyes principle” -** AutoNSX creates all nececary changes in Service Now ITSM fulfilling it with all objects applied to the VMware NSX distributed firewall. Those are approved by Application Owners their delegates and/or by the security team. At any given time, all history of changes applied to NSX can be seen in AutoNSX. The report shows, who, when and what was changed. This functionality exists only in AutoNSX.

The AutoNSX Software Solution Prevents “blindfold” policy implementations – no one does it!

Many Software Security Solutions can provide visibility on traffic flows and patterns which are used as a base to build security policies. However, those tools are blind to the traffic legitimacy. Users are asked to implement the security policies and then to run expensive analytics tool on top of the policy, which make TCO extremely poor.

AutoNSX takes different approach by allowing users (Security Architect, Security Engineer, SecOps) to define well know malicious IP address lists in AutoNSX before the security policy implementation. IP address list can be simply copy/paste or loaded via CSV files in newer version this list is automatically populated. Security Architect, Security Engineer, SecOps then defines the desired condition against the list, for example: highlight in the segmentation report if the IP is part of the malicious list, or even prohibit segmentation to be executed. This results to a very strict security and prevent malicious IPs to be added to the firewall. While executing application segmentation DevOps will be notified if the malicious IP is part of the any traffic flow. DevOps team can export the report and start investigation before implementing the security policy.



Contact us:

Druzhba 26 str, Varna, 9000 Bulgaria
info@digitout.net
+359 899 341 203

FREE TRIAL BOOK DEMO