tufin The Security Policy Company. + vmware NSX PARTNER

Technology Partner Solution Brief

VMware NSX with Unified Security Management from Tufin

Benefits to Your Business:

- Comprehensive visibility, analysis and automation for security policies in NSX-v and NSX-T
- Simplify the migration from NSX-v to NSX-T by leveraging a central solution that supports both
- Increase agility with end-to-end change automation across NSX, physical firewalls and routers and public cloud platforms
- Design, enforce, and manage micro-segmentation across vendors and platforms in the physical and virtual network
- Manage application connectivity uniformly across NSX and other platforms
- Reduce audit preparation time by up to 70% and enforce continuous compliance with corporate policies and industry regulations
- Visualize and troubleshoot network connectivity across the heterogeneous network
- Control security policies from NSX DFW, routers,and edge devices and leading enterprise firewalls and cloud platforms from a single pane of glass

SDN Approach Re-Envisions Network Security

The Software-Defined Network (SDN) enables a substantially improved operational mode with greater agility, higher control over security, lower operational overhead, and a lower capital expenditure model.

VMware NSX delivers network virtualization for the SDN, with a full service, programmable platform that provides a logical network abstraction of the physical network with programmatic provisioning and management abilities. VMware NSX redefines the way we secure our networks. One of the fundamental challenges of network security has been the inability to isolate policy enforcement from the operational network plane. Within the SDN, the hypervisor provides a perfectly isolated layer to enforce security policy while maintaining the application context to enable better security control and visibility.

NSX provides isolation and network segmentation by default using the Distributed Firewall (DFW). Virtual networks run in their own address space and have no communication path to each other or to physical networks. Native firewalling and policy enforcement at the virtual layer provides a method to design and deploy segmentation. Micro-segmentation is made manageable through applying security controls at the unit level or virtual machine level, or most often to Security Groups.

The SDN enables security to be architected into the network itself. This allows security controls to be based on logical boundaries and makes data center micro-segmentation operationally feasible. However, as most organizations rely on more than one network platform, the ability to realize the full benefits of the SDN in addition to the rest of network requires a solution to make network security manageable and agile.

Tufin Orchestration SuiteTM Solution for VMware NSX

Tufin Orchestration Suite is a complete solution for automatically designing, provisioning, analyzing, and auditing network security policy changes. IT and security teams centrally design, deploy, and manage micro-segmentation, continuously monitor and track security policy compliance, and automate security policy management throughout the entire hybrid network via a single pane of glass. Tufin Orchestration Suite provides unprecedented visibility and control of security in the SDN, the legacy network, and the public cloud. Tufin offers full support for both NSX-v and NSX-T and simplifies the migration of enterprise customers from one to the other.

Automatic Change Design, Provisioning, Verification, and Tracking

Tufin Orchestration Suite offers a change designer that provides the automatic design of the most efficient network access path while ensuring continuous adherence to security policy when making changes to the network. Through the integration with VMware NSX, the designed changes are automatically provisioned across the NSX DFW Security Groups, legacy network devices, and public cloud. Automated provisioning ensures that configuration changes are implemented across the devices in the path accurately and quickly and verification ensures connectivity was established. All changes are fully documented and readily retrievable for audit.

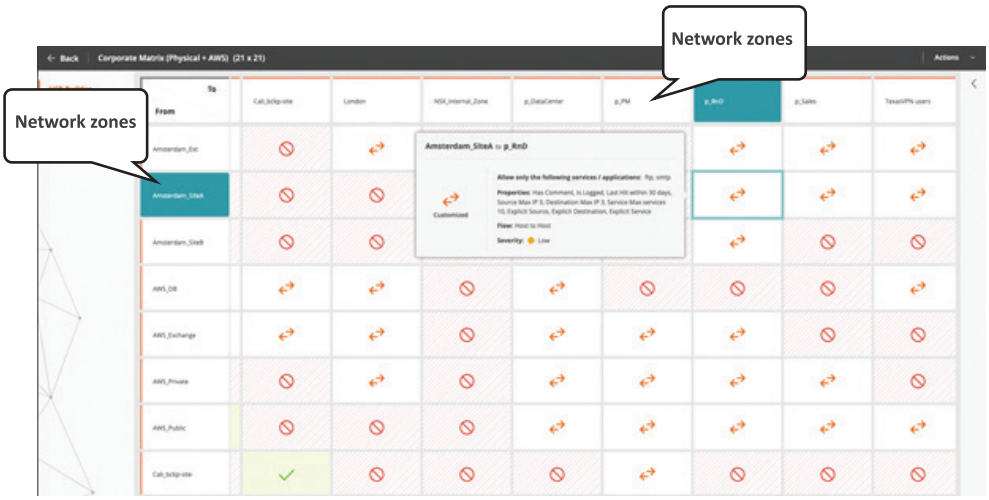
Micro-Segmentation

The integration of VMware NSX and Tufin Orchestration Suite delivers a consolidated dashboard to manage and continuously validate compliance with network security policy. Tufin Unified Security Policy enables customers to visually map network zone-to-zone traffic flows and instantly gain insights and visibility for micro-segmentation between IPs, subnets, and Security Groups.

After defining your desired micro-segmentation mapping, Tufin Orchestration Suite identifies and alerts on segmentation violations in real time and provides on-going control with proactive security checks integrated into the change process.

Security Policy Management

Tufin Orchestration Suite unifies and centralizes control of security policies across the entire data center, supporting the leading enterprise security vendors across physical, virtual networks, and hybrid cloud. It enables continuous monitoring and alerting for security policy configuration changes. And provides policy analysis and optimization. With change tracking and reporting, IT and security managers gain full visibility and documentation for security configuration changes across one or more NSX instances – providing a clear and definite answer to who did what, when and why, and what is the security and compliance impact of every change.



Tufin Orchestration Suite Unified Security Policy – enables central management of network segmentation to ensure continuous compliance

Summary

VMware NSX together with Tufin Orchestration Suite provides a unified plane of visibility and control to IT and security professionals responsible for a complex network that includes the SDN. The joint solution enables customers to reap the benefits of the SDN while ensuring consistent adherence to security policy, and to manage approachable and actionable micro-segmentation – throughout the SDN, and across the physical network and public cloud.

tufin The Security Policy Company.

Tufin (NYSE: TUFN) simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the company's Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Tufin Orchestration Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. With over 2000 customers since its inception, Tufin's network security automation enables enterprises to implement changes in minutes instead of days, while improving their security posture and business agility. Find out more at **www.tufin.com**.

vmware NSX PARTNER

VMware software powers the world's complex digital infrastructure. The company's compute, cloud, mobility, networking and security offerings provide a dynamic and efficient digital foundation to over 500,000 customers globally, aided by an ecosystem of 75,000 partners. Headquartered in Palo Alto, California, this year VMware celebrates twenty years of breakthrough innovation benefiting business and society.
For more information, please visit https://www.vmware.com/company.html.