VMware NSX with Unified Security Management from Tufin

Solution Brief

Highlights

The integrated VMware NSX™ and Tufin Orchestration Suite™ delivers unified security policy management across physical and virtual networks within the Software-Defined Data Center (SDDC). It enables IT organizations to:

- Manage and control micro-segmentation across physical, virtual and hybrid networks
- Centrally manage security policies on firewalls, routers and switches throughout the entire data-center via a single interface
- Assess the risk posture and perform risk assessment before making policy changes
- Perform real-time compliance monitoring, analysis and alerts on policy changes
- Continuously track security policy configuration change across virtual and physical networks
- Reduce audit preparation time by up to 70%.

Redefining Network Security within the SDDC

The Software-Defined Data Center enables a substantially improved operational mode with greater speed and agility, lower operational overhead, and a lower capital expenditure model.

VMware NSX delivers network virtualization for the SDDC, with a full service, programmable platform that provides logical network abstraction of the physical network with programmatic provisioning and management abilities. Following the successful abstraction of the compute and storage elements, network virtualization provides the next step towards a fully virtualized data center.

VMWare NSX also offers an opportunity to redefine 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 SDDC, 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. 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 segmentation, and micro-segmentation for security controls at the unit level or virtual machine level.

Leveraging network virtualization technology, the SDDC provides the opportunity to re-architect and improve network security, ensuring that it is optimized for the computing environment and infrastructure of the SDDC.

The Tufin Orchestration Suite for VMware NSX

NSX is a distributed service platform that enables dynamic service insertion of advanced services like Tufin Orchestration Suite. The Tufin Orchestration Suite is a complete solution for automatically designing, provisioning, analyzing and auditing network security changes from the application layer down to the network layer.

With the Tufin Orchestration Suite, IT and security organizations can centrally manage and control micro-segmentation, continuously monitor and track security policy compliance, and automate security policy management throughout the entire data-center via a single interface. The Tufin Orchestration Suite provides unprecedented visibility into and control over SDDC security; ensuring a unified security policy management across physical, virtual and hybrid networks within the SDDC.

Cross Data Center Micro-Segmentation

The joint solution featuring VMware NSX and the Tufin Orchestration Suite delivers automation and visibility that significantly reduces the management burden of micro-segmentation across physical and virtual networks. With Tufin's Security Zone Matrix you can visually map network zone-to-zone traffic flows and instantly gain insights and visibility to your micro-segmentation, across physical, virtual and hybrid networks (see Figure 1).

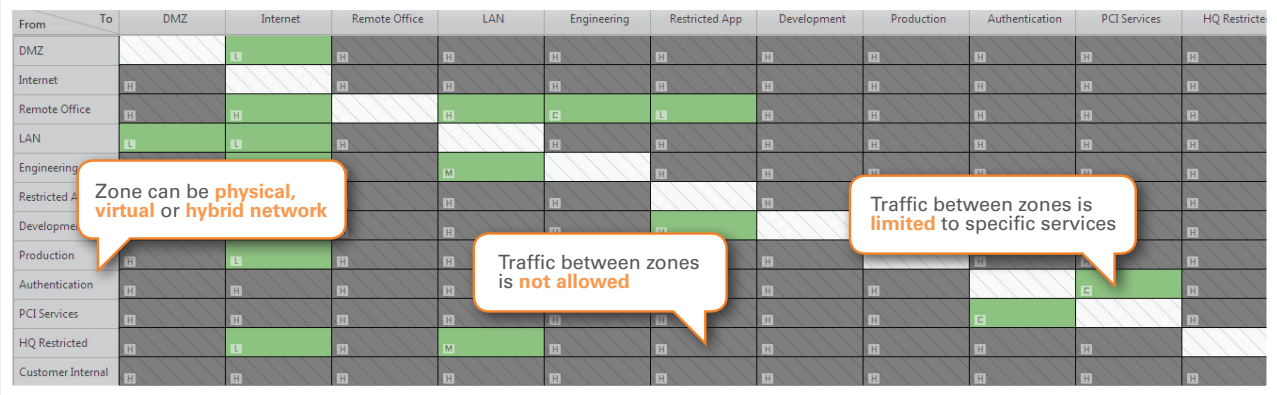


Figure 1: Tufin's Security Zone Matrix

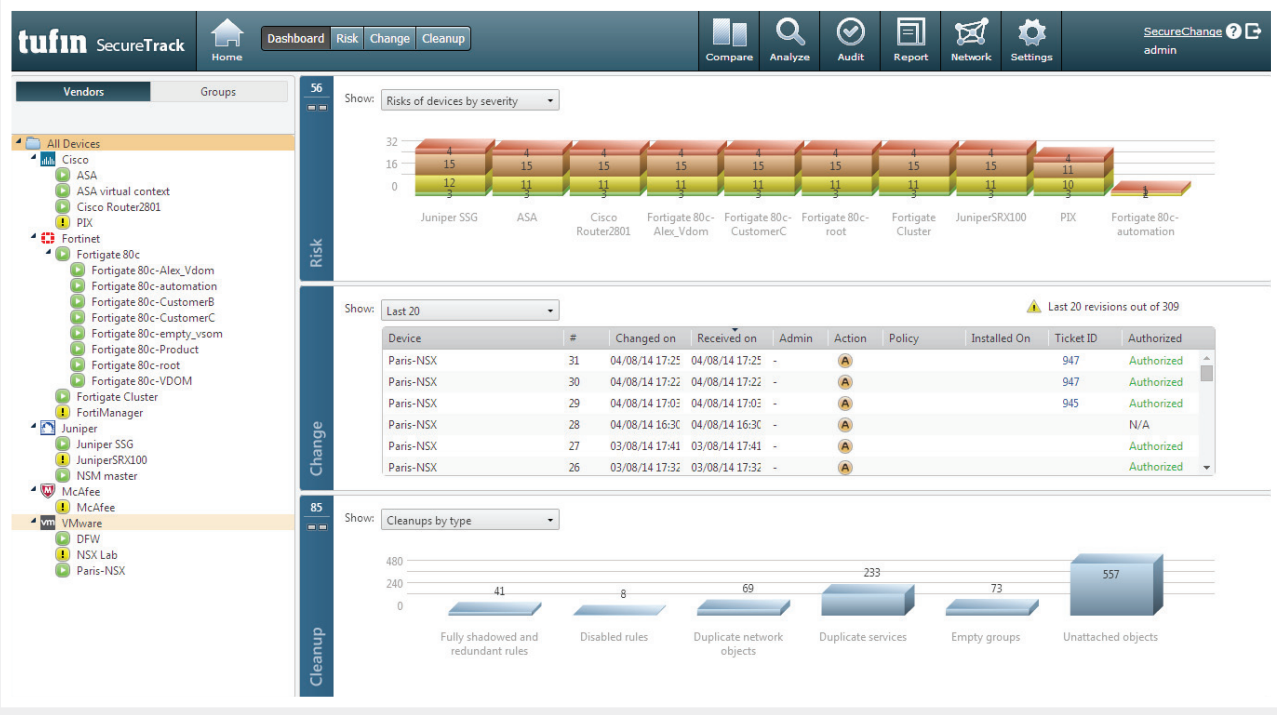
After defining your desired micro-segmentation mapping, the Tufin Orchestration Suite helps you easily identify segmentation violations, and gives you on-going control with integrated security checks as part of the change process.

Data-Center Compliance Management

The Tufin Orchestration Suite enables IT and security organizations to centrally manage security policy compliance and compliance violations across the entire data-center, via a single unified interface. With out-of-box regulatory compliance reports and real-time alerts on compliance violations, IT and security organizations can slash audit preparation time and assure continuous compliance.

Unified Security Policy Management

The Tufin Orchestration Suite™ unifies and centralizes control of security policies across the entire data center, supporting the leading enterprise security vendors across physical, virtual and hybrid networks. It enables continuous monitoring and alerting for security policy configuration changes across physical and virtual firewalls, routers and switches. With change tracking and change visualizations, IT and security managers gain full accountability for security configuration changes – providing a clear and definite answer to who did what, when and why, and what is the security and compliance impact of every change.



Summary

VMware NSX with the Tufin Orchestration Suite provide a unified plane of visibility and control to IT professionals who are planning to deploy a software-defined data center. The joint solution enables IT and security organizations to reap the benefits of the SDDC while ensuring consistent security behavior and micro-segmentation policies throughout the data center, across both physical and virtual networks.

www.tufin.com

SB-8-14