

VMware NSX und Unified Security Management von Tufin

Die Lösung unseres Technologiepartners im Überblick

SDDC erhöht die Netzwerksicherheit in Rechenzentren

Das softwaredefinierte Rechenzentrum (SDDC) bietet einen erheblich effizienteren Betrieb mit schnelleren Prozessen, größerer Agilität und geringeren Betriebs- und Investitionskosten.

VMware NSX ist eine programmierbare Full-Service-Plattform für die Netzwerkvirtualisierung im SDDC, die eine logische Abstraktion des physischen Netzwerks mit programmatischen Bereitstellungsoptionen und Verwaltungsfunktionen ermöglicht. Nach der Abstraktion von Computer- und Storage-Komponenten ist die Netzwerkvirtualisierung der nächste Schritt zum vollständig virtualisierten Rechenzentrum.

Mit VMware NSX kann darüber hinaus der Netzwerkschutz neu definiert werden. Eine der größten Herausforderungen bei der Netzwerksicherheit stellte bisher die Tatsache dar, dass die Durchsetzung von Richtlinien nicht vom Netzwerkbetrieb getrennt werden konnte. Im SDDC stellt der Hypervisor eine vollständig isolierte Schicht zur Durchsetzung der Sicherheitsrichtlinien dar und behält gleichzeitig den Anwendungskontext bei, um für eine bessere Sicherheitskontrolle und mehr Transparenz zu sorgen.

NSX ermöglicht standardmäßig die Isolierung und Netzwerksegmentierung. Virtuelle Netzwerke arbeiten jeweils in ihrem eigenen Adressraum und verfügen über keinen Kommunikationspfad zueinander oder zu physischen Netzwerken. Eine native Firewall und die Durchsetzung von Richtlinien auf der Virtualisierungsebene ermöglichen die Segmentierung und Mikrosegmentierung für Sicherheitskontrollen auf der Stufe von Rechnern oder virtuellen Maschinen.

Mithilfe von Netzwerkvirtualisierung werden im SDDC Sicherheitsfunktionen in das Netzwerk selbst integriert. Die Sicherheitskontrollen basieren dementsprechend auf logischen Grenzen, und eine Mikrosegmentierung des Rechenzentrums wird ermöglicht.

Die Tufin Orchestration Suite™ für VMware NSX

Die Tufin Orchestration Suite ist eine Komplettlösung für die automatische Planung, Bereitstellung, Analyse und Prüfung von Änderungen an Sicherheitsrichtlinien im Netzwerk – von der Anwendungsbis zur Netzwerkschicht.

Die Tufin Orchestration Suite bietet IT- und Sicherheitsabteilungen eine zentrale Oberfläche zur Verwaltung und Steuerung von Mikrosegmentierungen, zur kontinuierlichen Überwachung und Verfolgung der Richtlinien-Compliance sowie zur einheitlichen Verwaltung von Sicherheitsrichtlinien im gesamten Rechenzentrum. Durch die zentrale Steuerung von Sicherheitsrichtlinien im gesamten Unternehmen – einschließlich physischer und virtueller Netzwerke sowie Hybrid-Cloud-Plattformen – ermöglicht die Tufin Orchestration Suite beispiellose Transparenz und Kontrolle über die Sicherheit im SDDC.

Rechenzentrumsübergreifende Mikrosegmentierung

Dank der Automatisierung und umfassenden Transparenz, die eine Kombination von VMware NSX mit der Tufin Orchestration Suite bietet, wird der Verwaltungsaufwand für die Mikrosegmentierung von physischen und virtuellen Umgebungen erheblich reduziert. Mit der Sicherheitszonenmatrix von Tufin kann der Datenverkehr von Zone zu Zone visuell abgebildet werden, sodass Sie eine Übersicht über die Mikrosegmentierung in Ihrem Unternehmen erhalten (siehe Abbildung 1).

Highlights

Eine integrierte Lösung aus VMware NSX™ und der Tufin Orchestration Suite™ ermöglicht eine zentrale Verwaltung von Sicherheitsrichtlinien und Compliance in physischen und virtuellen Netzwerken sowie der Hybrid Cloud. Sie bietet IT-Abteilungen folgende Vorteile:

- Steuerung der Mikrosegmentierung von physischen, virtuellen und hybriden Netzwerken
- Nachverfolgung von Änderungen an Sicherheitsrichtlinien auf führenden Cloud-Plattformen und Unternehmensfirewalls, einschließlich verteilter NSX-Router und Edge-Geräten
- Kontinuierliche Compliance und Reduzierung der Vorbereitungszeit für Audits um bis zu 70 %
- Visualisierung von Richtlinien und Netzwerkonnektivität im heterogenen Unternehmensnetzwerk
- Zentrale Überwachung und Verwaltung der Anwendungskonnektivität auf NSX- und anderen Plattformen

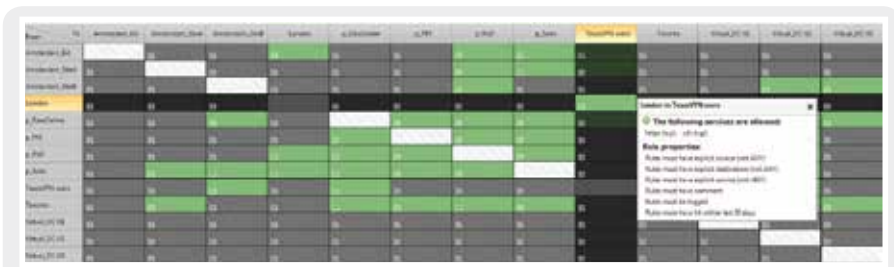


Abbildung 1: Sicherheitszonenmatrix von Tufin

Wenn Sie die gewünschte Mikrosegmentierung festgelegt haben, unterstützt Sie die Tufin Orchestration Suite bei der Erkennung von Schutzverletzungen und ermöglicht Ihnen eine kontinuierliche Kontrolle dank integrierter Sicherheitsprüfungen im Rahmen des Änderungsprozesses.

Compliance-Management für das Rechenzentrum

Mit der Tufin Orchestration Suite können IT- und Sicherheitsabteilungen die Einhaltung von Sicherheitsrichtlinien im gesamten Rechenzentrum über eine zentrale Oberfläche steuern. Dank sofort nutzbarer Compliance-Berichte und Echtzeitwarnungen bei Compliance-Verstößen können IT- und Sicherheitsabteilungen die Vorbereitungszeit für Audits deutlich reduzieren und lückenlose Compliance gewährleisten.

Zentrale Verwaltung von Sicherheitsrichtlinien

Die Tufin Orchestration Suite vereinheitlicht und zentralisiert die Verwaltung von Sicherheitsrichtlinien im gesamten Rechenzentrum. Sie unterstützt die führenden Anbieter von Sicherheitslösungen für physische und virtuelle Netzwerke sowie Hybrid-Cloud-Lösungen in Unternehmen. Zudem ermöglicht sie die kontinuierliche Überwachung und Meldung von Änderungen an der Sicherheitskonfiguration auf physischen und virtuellen Firewalls und Cloud-Plattformen. Durch die Verfolgung und Visualisierung von Änderungen profitieren IT- und Sicherheitsabteilungen von vollständiger Transparenz der Sicherheitskonfigurationen in einer oder mehreren NSX-Instanzen: Sie können den Urheber, die Ursache und den Zeitpunkt jeder Änderung genau identifizieren, einschließlich ihrer Auswirkungen auf Sicherheit und Compliance.



Abbildung 2: Dashboard der obersten Ebene von Tufin

Rechenzentrums- und Anwendungsmigration

Die Tufin Orchestration Suite vereinfacht die Migration von Anwendungen und ermöglicht dabei eine Netzwerksegmentierung in physischen sowie SDDC- und Cloud-Infrastrukturen ohne Unterbrechung der Betriebsabläufe. Ein automatischer Erkennungsalgorithmus zur Visualisierung der Anwendungskonnektivität sowie die Planung und Bereitstellung von Änderungen an Sicherheitsrichtlinien vereinfachen und beschleunigen die Migration im Rahmen eines Wechsels zum SDDC.

Zusammenfassung

VMware NSX und die Tufin Orchestration Suite schaffen eine zentrale Übersichts- und Kontrollebene für IT-Experten, die ein softwaredefiniertes Rechenzentrum implementieren möchten. Mit dieser gemeinsamen Lösung können IT- und Sicherheitsteams die Vorteile eines SDDC nutzen und gleichzeitig im gesamten Rechenzentrum ein konsistentes Sicherheitsverhalten und einheitliche Richtlinien für die Mikrosegmentierung von physischen und virtuellen Netzwerken sowie Hybrid-Cloud-Umgebungen sicherstellen.

Tufin auf einen Blick

Niederlassungen: Nordamerika, Europa und Asien-Pazifik-Raum

Kunden: Mehr als 1.700 in über 50 Ländern

Führende Branchen: Finanzdienstleistungen, Telekommunikation, Energie- und Versorgungswirtschaft, Gesundheitswesen, Einzelhandel, Bildungswesen, Behörden, verarbeitende Industrie, Transportwesen und Auditoren

Vertriebspartner: Mehr als 240 weltweit

Technologiepartner und unterstützte Plattformen: Amazon Web Services, BMC, ServiceNow, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Forcepoint™, Juniper Networks, Microsoft Azure, OpenStack, Palo Alto Networks, VMware und andere