tufin The Security Policy Company.

vmware

Operationalizing NSX Network segmentation in the Software-Defined Network

A Comprehensive Solution for Visibility and Management of Heterogeneous Security Controls in a Data Center

Software-defined networking (SDN) is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to direct traffic on the network and communicate with the underlying hardware infrastructure.

More than 15 years ago, server virtualization platforms revolutionized computing by decoupling compute from hardware. This unleashed a wide range of benefits, from reduced hardware costs to improved business agility, and ignited the firestorm of cloud computing as well.

Compute virtualization introduced the hypervisor, a new model for virtualizing server resources needed by applications to simplify operations and speed provisioning time. Virtualization has become the de-facto standard for achieving operational efficiency and agility in the data center today.

Considering SDN?

Evaluate:

- How can we maintain visibility and control across diverse and dynamic environments?
- How do we ensure consistent security behavior throughout the entire data center, across physical and virtual networks and cloud platforms, plus multiple vendors in the mix?
- How do we ensure cross data-center compliance and segmentation?
- Can we enable business agility and operational efficiency across heterogeneous environment?

Until recently, the networking component of the data center remained in the physical realm. Technology breakthroughs and the adoption of virtualized environments have increased the need for network virtualization—and indeed it is taking root. Now it's possible to reproduce switches, routers, firewalls and load balancers in software in the same way that the CPU, memory and storage have been rendered in software. SDN is designed to create and control virtual network or control a traditional hardware network with software.

The goal is to achieve the same operational efficiencies in the network as were achieved by the virtualization of physical servers, and to attain the same benefits: business agility, reduction in costs, configuration flexibility, provisioning automation, and programmability of capabilities. But there's another benefit that is critically important for today's enterprise computing—improved security. By virtualizing the network through SDN, it's possible to put more security and tighter controls closer to the assets they are intended to protect. This development is driving rapid adoption of network virtualization.

The market-leading platform for network virtualization today is VMware NSX™ (includes NSX-T and NSX-v). It solves the fundamental challenge of network security, which has been the inability to isolate policy enforcement from the operational network plane.

© Copyright 2020 Tufin. All rights reserved.

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 offers security by default, allowing network and security isolation, segmentation, and network segmentation with dynamic insertion of advanced security services.

The Tufin Orchestration Suite™ provides the necessary extension to the segmentation capabilities enabled by VMware NSX. This unifies security policy management across not only the virtual networks within the software-defined network but also the physical networks and public cloud platforms.
This paper outlines how IT and security organizations can use the Tufin Orchestration Suite to centrally manage and control network segmentation, continuously monitor and track security policy compliance, and automate security policy management throughout the entire data center via a single pane of glass.

An Overview of SDN for Network Security

The traditional network security model focuses on perimeter defense, as shown in Figure 1.
A typical enterprise configuration has a pair of firewalls protecting the data center from the external Internet under the assumption that everything that is potentially bad is coming from the outside. Therefore, companies focus their security at the point where outside traffic could enter the data center.

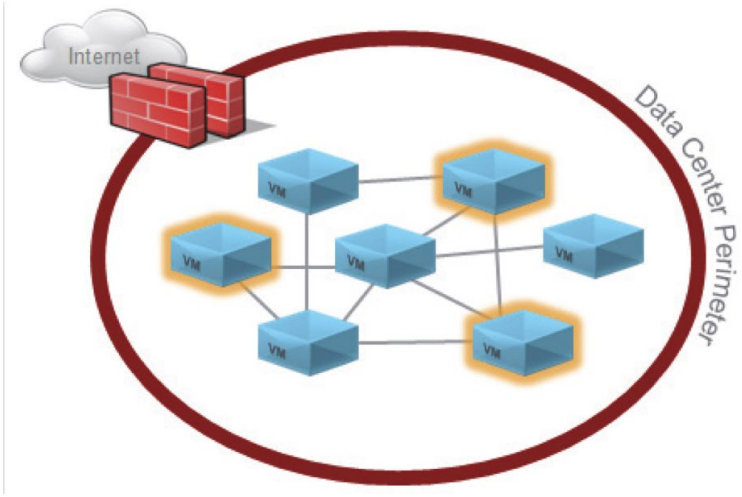

Figure 1: Network security at the perimeter

Traffic moving within the data center is usually not inspected, which means that it is possible to navigate from one server – physical or virtual – to another within the VM, without any security checks.
The problem here is that if one server gets infected with malware or is penetrated by an unauthorized party, the malware can easily spread to neighboring virtual servers, or the unauthorized actor can move from one server to another in search of high value targets. These scenarios have been found to be the most common pattern in numerous high-profile data breaches where the attacker has been able to move freely within the perimeter in search of critical assets.

The data center can be configured to possibly route traffic from a VM back through the perimeter firewall for inspection before sending it back inside to the data center. This approach will work; however, this additional overload of high volume interal data center traffic and rules creates a complex environment that will affect the efficiency of the perimeter firewalls . In the end, the perimeter security approach to securing VMs is inadequate as evidenced by the fact that the number of data center security breaches has not declined in recent years.

VMware recommends intrinsic security approach to secure your data center traffic, via network segmentation, as illustrated in Figure 2. Instead of having just one firewall located at the perimeter to secure and enforce policies, each VM within the

© Copyright 2020 Tufin. All rights reserved.

data center is now protected with its own firewall which runs the entire set of security capabilities for any traffic going through the firewall or alternatively NSX Service-defined Firewalls can be deployed to secure the VMs. Due to the position of NSX-T Edge within NSX-T, the NSX-T Gateway Firewalls is also able to secure traffic for various patterns including following types of communication between: [1]

- Virtual workloads and physical servers
- Physical server to physical server
- Segmented communication between tenant segments and their virtual workloads

This ensures that the traffic traversing between the data center as well as crossing the perimeter now doesn't have to be diverted through the perimeter firewall for security inspection. From a security perspective this is a great model, but it is only feasible through the technology of a software-defined networking. This model of placing individual firewalls at every server is impractical due to the sheer number of firewalls that would be required and the complex routing instructions. In aggregate this approach would be an operational nightmare, not to mention that it would be cost prohibitive.

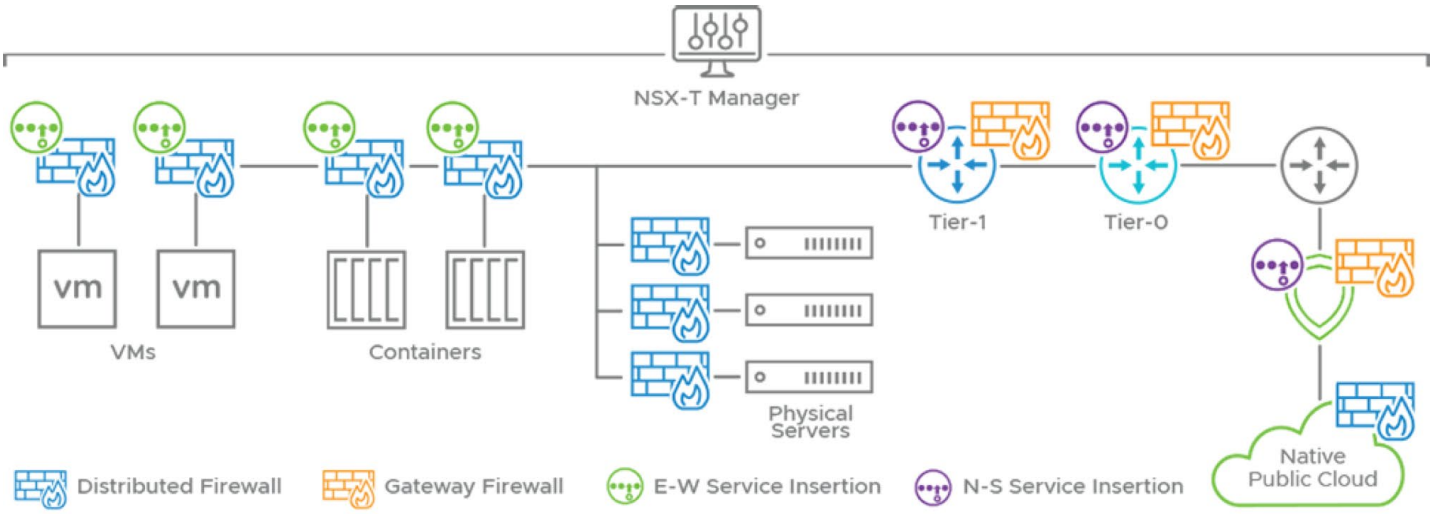

Figure 2: Network security via segmentation

Network segmentation provides numerous benefits. It allows granular, distributed controls and reduces the attack surface. It allows security administrators to see "east-west" traffic going between the VMs, which was not visible previously. It blocks harmful lateral movement within the virtual environment so that even if one device is compromised, further proliferation of the attack can be stopped. In short, network segmentation enables a Zero Trust Model in which every piece of traffic that traverses the data center is inspected, regardless of its origin.

There are multiple use cases for network segmentation. In the most basic sense, it can be used to isolate different environments, for example, to separate development, test and production environments from each other by allowing no communication paths among them, or to isolate payment systems from all other parts of a network as required by the PCI regulations.

1 https://blogs.vmware.com/networkvirtualization/2018/05/extending-the-power-of-nsx-to-bare-metal-workloads.html/

© Copyright 2020 Tufin. All rights reserved.

More interesting use cases take advantage of the virtual firewall's capabilities to scrutinize traffic between different VMs of the same environment. For example, a firewall can check the traffic going among web, application and database VMs. This can be fully controlled using the NSX security technologies and the NSX built-in distributed firewalls. Additional security controls can be plugged into the advanced segmentation scenario as well, such as inbuilt IPS, and IDS capabilities of NSX and other security technologies like AV or DLP. So, for instance, it's possible to put a data loss prevention virtual device around a database containing sensitive data that requires strong protective measures.

With NSX, a security policy can be run within the hypervisor level so that any traffic that goes through any VM is inspected the moment it hits a virtual wire, as shown in Figure 3. As soon as the VM tries to communicate with anything inside or outside the virtual environment, that traffic is immediately detected on the virtual NIC layer—right when it hits the hypervisor and is being inspected by the NSX distributed firewall. Moreover, once an administrator defines a security policy for a VM, this policy remains attached to that VM regardless of where it is located. If this VM moves, then the security policy moves with it. This happens in a completely automated way.

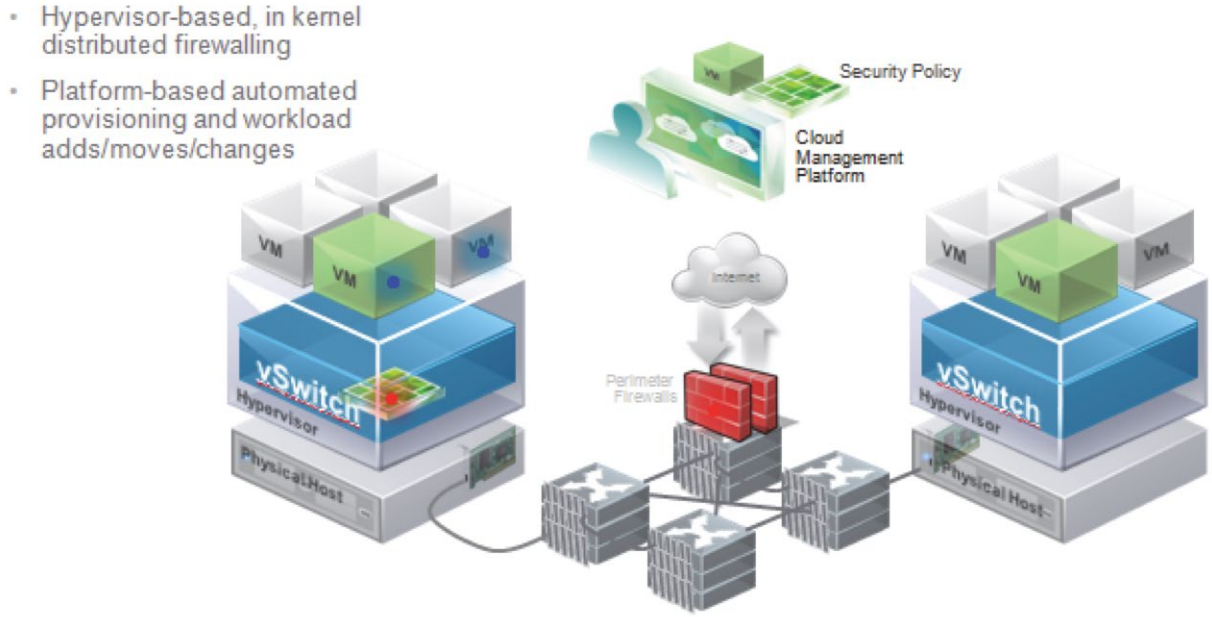

Figure 3: Security policy runs within the hypervisor level

The NSX platform (NSX-T) can now use its Distributed Firewall product for deeper inspection on traffic going inside the data center, between VMs. VMware NSX Service-defined Firewall is a stateful firewall, meaning it monitors the state of active connections and uses this information to determine which network packets to allow through the firewall. VMware NSX Service-defined Firewall is implemented in the hypervisor and applied to virtual machines on a per-vNIC basis. That is, the firewall rules are enforced at the vNIC of each virtual machine.

The NSX Service-defined Firewall provide next generation firewall capabilities, which provide the ability to create Ethernet rules (L2 rules) and General rules (L3 to L7 rules). Each VM has its own firewall policy rules and context.

© Copyright 2020 Tufin. All rights reserved.

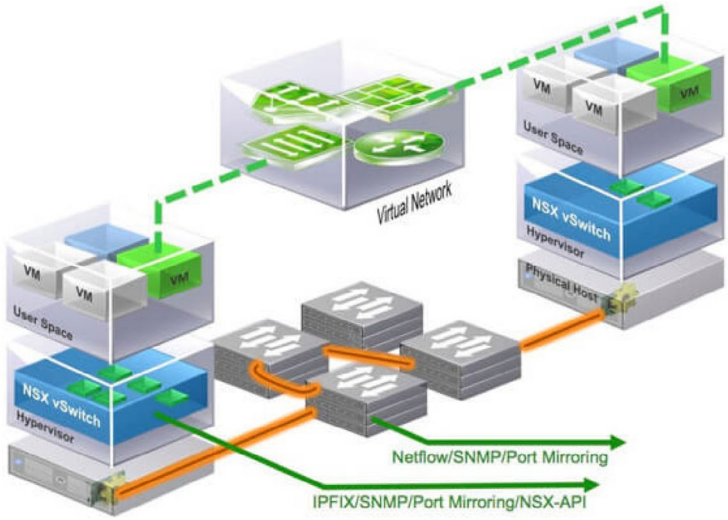

Figure 4: Traffic steering utilizing multiple virtual firewalls

In this example, the administrator defines a communication between virtual machines in a data center through VMware NSX Service-defined Firewall[2] and edge devices. With Tufin Orchestration Suite, these devices can be adapted to enforce security policies identical to the physical appliances that control the North-South traffic to the data center. When a VM sends traffic and it hits the hypervisor, this traffic is first inspected by the NSX Service-defined Firewall and traffic steering decision is made depending on whether the request can be redirected internally to the recipients inside the data center or steered to the third-party physical edge firewall for additional security screening. It's possible to connect different types of security devices and policies, one after another, to create layered security. This service chaining capability is a significant feature of VMware NSX.

Here's one more common use case for network segmentation. A traditional data center or a traditional DMZ typically has different VLANs with applications from different organizations sitting on the same network. This is illustrated in Figure 5. If, for example, the IT VLAN is infected, then in fact it is the entire DMZ VLAN which is now vulnerable. The idea of network segmentation is to be able to segment the network so that each application is completely segmented from the other applications. Thus, even if the IT VLAN is infected, it will not affect any of the other virtual networks within the DMZ. This stops lateral movement and ensures that the compromised device remains the only one that is affected.

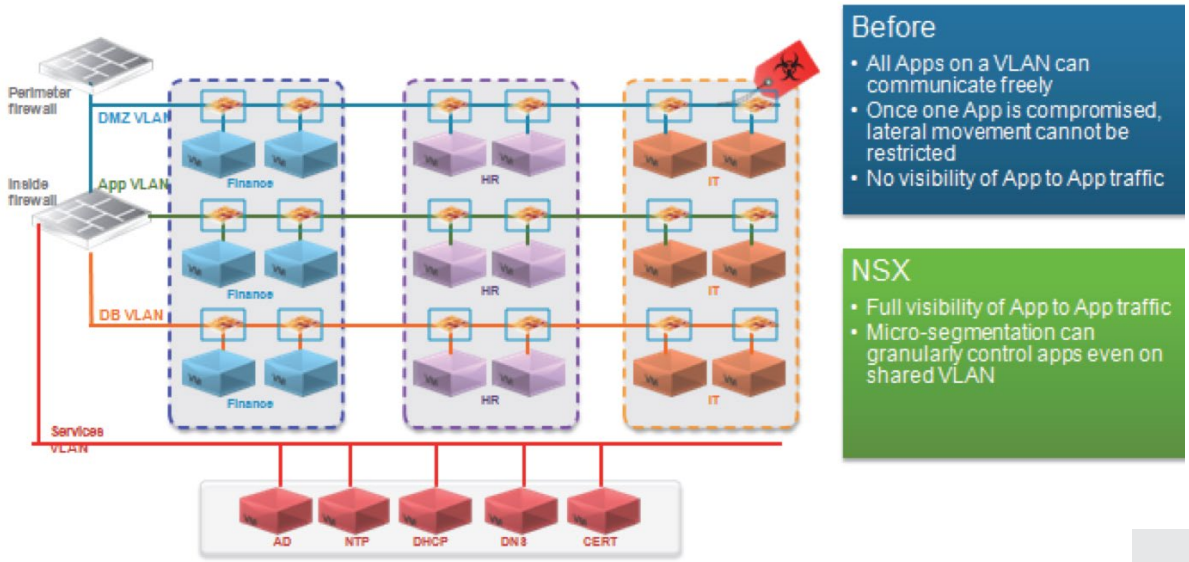

Figure 5: Network segmentation to protect VLANs

2 https://www.vmware.com/security/internal-firewall.html

© Copyright 2020 Tufin. All rights reserved.

In the high-profile breaches like Target Corporation, the attackers used a vulnerable device and then from that device started traversing the network laterally, jumping from one network to another until they gain access to the critical information they were seeking. Micro-segmentation would block such an event from occurring because each VM traffic is completely inspected, for security policy violations, by its own virtual firewall. As a result, if one VM is infected, an attacker cannot use that same physical network to move to other VMs in the same data center.In the high-profile breaches like Target Corporation, the attackers used a vulnerable device and then from that device started traversing the network laterally, jumping from one network to another until they gain access to the critical information they were seeking. Micro-segmentation would block such an event from occurring because each VM traffic is completely inspected, for security policy violations, by its own virtual firewall. As a result, if one VM is infected, an attacker cannot use that same physical network to move to other VMs in the same data center.

Security Management in the Software Defined Network

Enterprise environments are heterogeneous with the SDN being embedded in a larger environment that still consists of many physical networks and devices, along with cloud platforms (public, private, and hybrid) adding to this complexity. The data center is likely comprised of virtualized firewalls from VMware (i.e., the VMware NSX Service-defined Firewall); virtualized firewalls, NSX-T Gateway Firewalls to secure your VMs and bare metal and other edge security devices from third-party vendors like Palo Alto Networks, Check Point and Fortinet; and the traditional network components from vendors such as Cisco, Juniper Networks and F5 Networks.[3]

There are several main security management challenges pertaining to the SDN: network and segmentation, policy management and compliance, and migration to the SDN. Some of them are listed below:

Visibility and management of network segmentation

Organizations need to be able to manage segmentation both internal and external to the NSX environment. Network segmentation provides better security by tightening the security controls around a server (Physical and/or virtual machine or bare metal) when compared to traditional security controls, which are based on subnet segmentation. Operationalizing network segmentation requires effective configuration and managed. Accurate configuration of the NSX segmentation is crucial to take advantage of this innovative technology. This includes avoiding unnecessarily exposure of servers when deploying changes, and ensuring that business applications always have full connectivity.

Managing policies and compliance

Organizations need to manage their policies centrally—even though the policies might pertain to different platforms from different vendors on physical, virtual or cloud-based platforms. Security managers need broad and unified visibility. They need an audit trail of all changes, including advanced analysis and reporting capabilities, and they need to ensure that policies comply with the regulatory requirements that encompass their business.

Policy and change management becomes even more complicated if an organization needs to look at policy changes across multiple, heterogeneous platforms and conduct "what if" analysis for both the north-south traffic as well as the east-west traffic. For example, suppose a security administrator wants to assess if traffic is allowed between a VM and a physical asset outside of the SDN. The administrator needs to understand the security devices the traffic is going to pass through and simulate the traffic pattern if such a change is implemented. This will help them to understand if the traffic will be accepted or dropped even before they can deploy the actual change.

In a more advanced scenario, the administrator is assessing the case of traffic moving between two VMs and this traffic is going to be inspected by both the VMware distributed firewall policy and a third-party external firewall that is running right after using the traffic steering. This is complicated, especially in an environment of service chaining where different sets of policies rely on different technologies and vendors' devices.

3 https://blogs.vmware.com/networkvirtualization/2018/05/extending-the-power-of-nsx-to-bare-metal-workloads.html/

 © Copyright 2020 Tufin. All rights reserved.

The Tufin Orchestration Suite Helps to Operationalize Network Segmentation

The Tufin Orchestration Suite creates a Unified Security Policy layer across the entire enterprise network and its data centers. The suite is comprised of several components that interact with each other as well as with the network infrastructure and the business applications. The suite also supports APIs to communicate with other important elements of the computing environment. The architecture of this suite is illustrated in Figure 6.

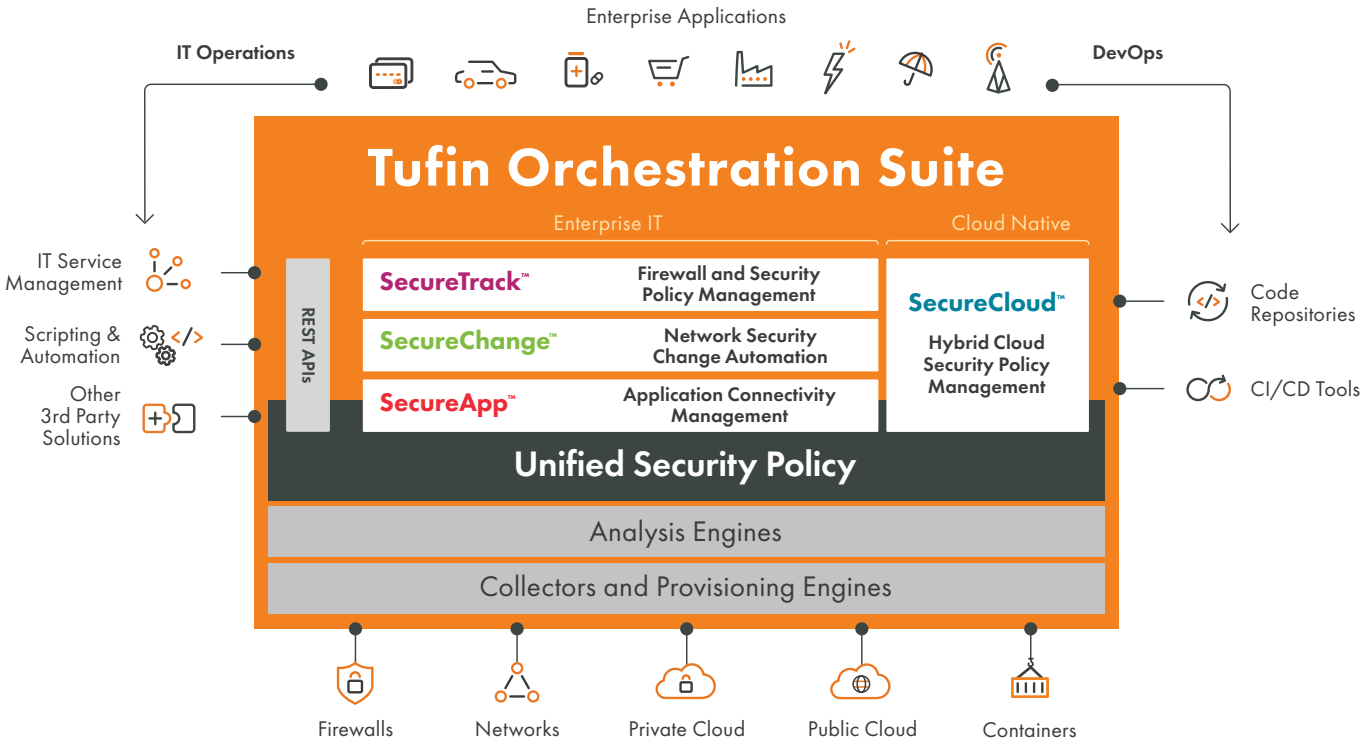

Figure 6: The architecture of the Tufin Orchestration Suite

Briefly, here's a description of each of these component's functionality:

- The Enterprise applications are the core applications that an organization provides to its customers and other stakeholders with products and services to fulfil their business needs.
- These applications are supported by diverse multi-vendor network components and infrastructure to efficiently provide such services to the end-user. We usually encounter two types of applications in most organizations:
- Tightly controlled applications where every change needs to be vetted against a security or compliance policy before it is implemented in the production.

  Tickets flow from application developers through ticketing systems such as ServiceNow or BMC Remedy into the Tufin Orchestration Suite. These changes are pro-actively checked with the Unified Security Policy for violations and processed through analysis engines to mimic the 'what-if' analysis to ensure business continuity.
- Cloud native applications are now at the forefront of the organizations undergoing digital transformations due to the agility presented by such infrastructures. In cloud native environments, developers and DevOps teams are instrumental in initiating access related changes. These teams are involved in designing East-West connectivity and might not have the oversight from the security teams.

© Copyright 2020 Tufin. All rights reserved.

How the Tufin Orchestration Suite Works in the SDN Environments

The Tufin Orchestration Suite provides granular management capabilities across the virtual, physical and cloud aspects of the network. The following sections outline how this is done.

Managing and enforcing network segmentation

Key Considerations:

There are three ways in which Tufin contributes to the management of network segmentation for the SDN.

1. Tufin takes a centralized approach to identifying and managing violations and exceptions.
2. Tufin provides a unified and consistent policy across both physical and virtual environments, with clear graphical visibility into that policy.
3. Tufin can automatically check any planned change against a segmentation policy before it is implemented to make sure that the change is not introducing a new policy violation.

Figure 7 shows the Tufin zone segmentation matrix which is an element of the Unified Security Policy. This matrix represents the different network zones on both the horizontal and vertical axis, and the blocks are color-coded to denote the communication permissibility status. For example, a green block represents that traffic between these two zones is allowed, but only for specific services. A gray block means that traffic is not allowed. A zone could span across physical, virtual or hybrid cloud platforms.

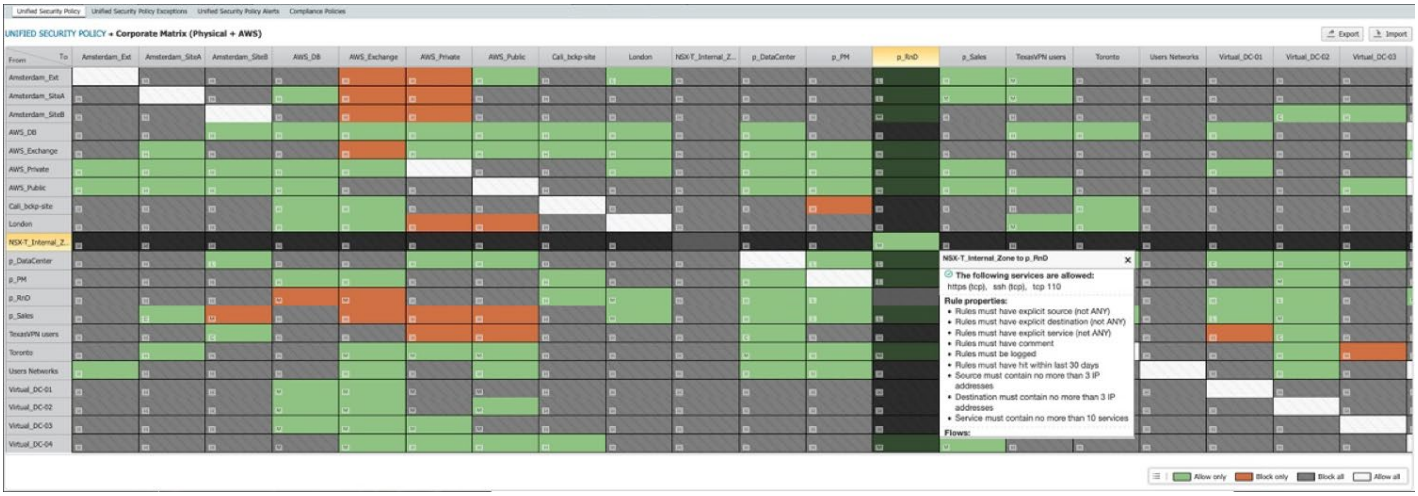

Figure 7: Tufin's segmentation management matrix

Once an organization has designed its desired segmentation policy using this visual matrix view, Tufin analyzes the network to see where there might be policy violations and to find the gaps between what is desired and what enforcement policy is running in the different policy enforcement points in the network - firewalls, routers and security groups. Unlike manual spreadsheets that security administrators typically create, this matrix is connected to the network and can automatically detect violations.

© Copyright 2020 Tufin. All rights reserved.

#	Device	Total Rules	Rule Status	Rule Count	Rule Count %	Critical	High	Medium	Low
Total:		68	Violating	13	19.1%	1	11	0	1
			Exempted	0	0%	0	0	0	0
1	NSX-DFW (NSX-Policy)	4	Violating	1	25%	0	1	0	0
			Exempted	0	0%	0	0	0	0
2	cpmodule (Standard_Prod)	40	Violating	12	30%	1	10	0	1
			Exempted	0	0%	0	0	0	0
3	PAN1	7	Violating	0	0%	0	0	0	0
			Exempted	0	0%	0	0	0	0
4	SRX-Bordeaux	17	Violating	0	0%	0	0	0	0
			Exempted	0	0%	0	0	0	0

Figure 8: A sample policy violation report

Operational requirements occasionally request visibility into exception to a desired segmentation policy; for example, to allow a specific business application access for business continuity, even though it may pose some risk to the organization. Tufin's Unified Security Policy has centralized exception management, as shown in Figure 9. A security administrator can manage the exceptions and assign them an expiration date so that the exceptions will have to be reexamined or removed after a specific date. This gives the security administrator time to discuss the requirements with the business application owner and design alternatives to keep the application in the service. All policy exceptions designed and architected through Tufin are automatically documented and are auditable.

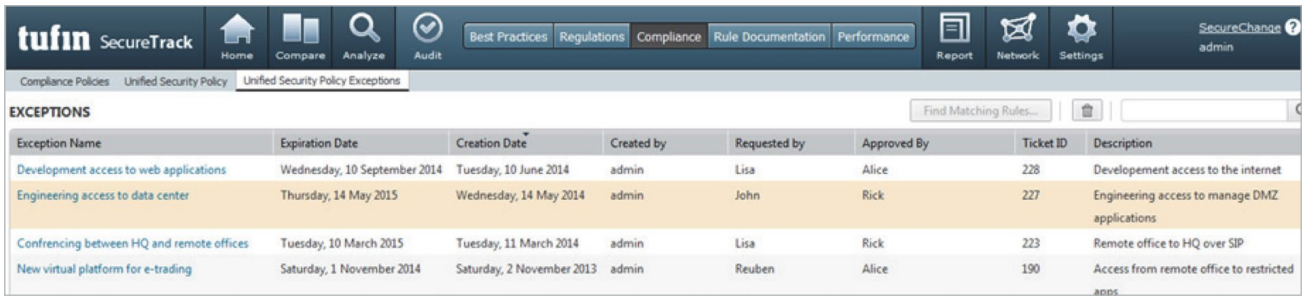

Figure 9: A sample exception report

The Unified Security Policy also proactively identifies potential violations of segmentation policy before the change is made. The change administrator request can decide either to add it as an exception or return it back to the requestor with a note regarding violation of the the segmentation policy.

Policy management and compliance

The Tufin Orchestration Suite supports policy management and compliance for the software-defined network in several ways. Tufin offers centralized management for multi-vendor technologies and can assure continuous automated regulatory compliance. The Unified Security Policy provides out-of-the-box common compliance reports. Tufin can help the security managers to have the same level of visibility and control in their new software-defined environment that they are accustomed to in a traditional data center environment. Policy management is fully automated with a comprehensive audit trail and documentation—so that all changes can be tracked, and reports can be produced for auditors on-demand. Figure 10 shows an example of change tracking of a security policy. There is a side-by-side comparison of the policy before and after the change. At any point it's easy to see who did what, when and why, and this can be fully documented for future reference. The left-side of this sample report also shows that different firewalls, virtualization platforms and cloud providers can all be managed from a single interface, sometimes referred to as "a single pane of glass."

© Copyright 2020 Tufin. All rights reserved.

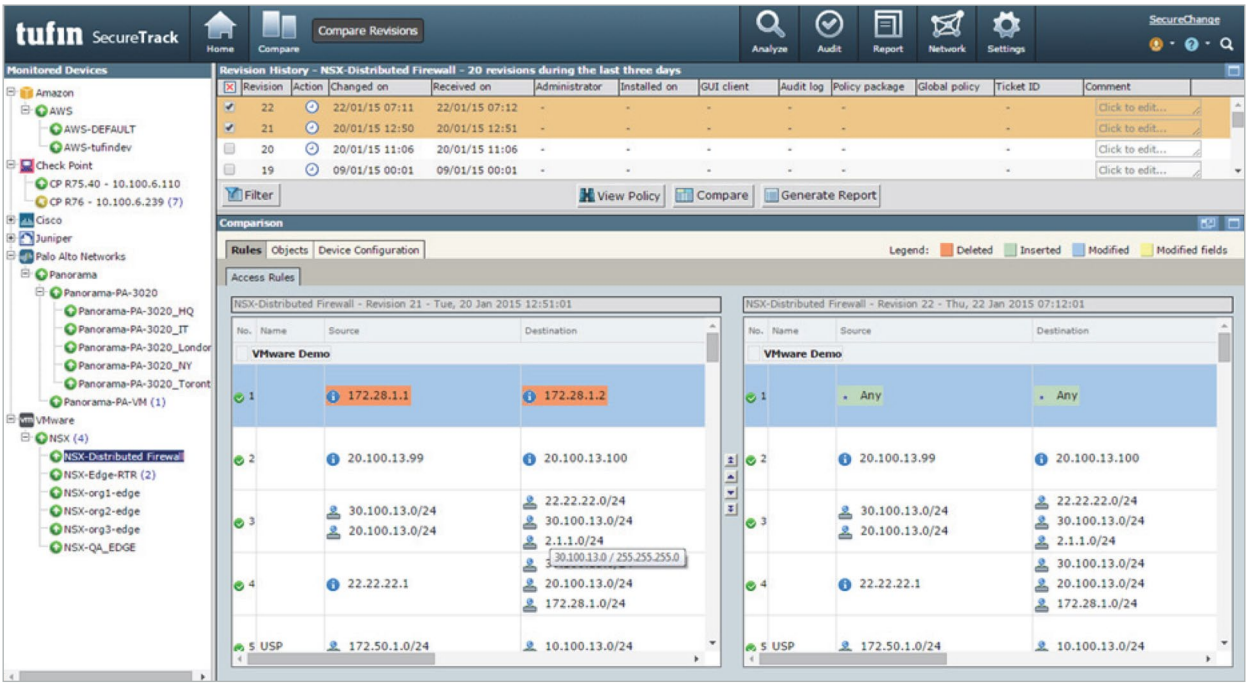

Figure 10: A "before" and "after" comparison of a policy change

There are overview and detailed violations reports for compliance policies such as PCI, SOX and other common industry regulations. The reports cover all security devices from NSX or third parties, whether they are physical, virtual or cloud based. Another important capability is the "what-if" policy analysis engine that investigates what would happen if certain types of rules were implemented. The Tufin Orchestration Suite can check if access is allowed from point A to point B and then check to see what route that potential traffic would take—i.e., which routers and firewalls this traffic would traverse. Tufin can determine whether the traffic would go through based on the existing security policies running on those firewalls and routers. This analysis can look at north-south as well as east-west traffic and takes into consideration both the virtual and the physical devices. Policy analysis assures that future changes are being checked for potential violations so that no new risk is being introduced into the environment. This capability is illustrated in Figure 11.

Figure 11: An example of "what-if" policy analysis

© Copyright 2020 Tufin. All rights reserved.

Managing NSX-v and NSX-T data centers side-by-side

Organizations have rapidly adopted the VMware NSX-v data centers to manage their application workloads efficiently through scale and high performance. With the launch of NSX-T the benefits of software defined network is now not limited to VMware components, customers can now design and architect data centers with hybrid and diverse technologies from public and private clouds to other hypervisors and physical workloads. Customers are focusing on deploying newer applications in NSX-T while continuing to maintain the NSX-v data center for their legacy applications. This introduces complexity as customer has to ensure security, visibility, orchestration and automation across two distinct and diverse data center operations. Tufin's comprehensive support for NSX-T and NSX-v will instill confidence in the customers to ramp up their operations in NSX-T while maintaining business continuity with existing data centers. Customer can be rest assured that the policies designed for the NSX-v data centers and other multi-vendor security devices in the network can now be applied and monitored uniformly with NSX-T data centers as well. So when the applications are deployed ground up, they will be compliant and will adhere to the security policies designed for the organization.

Outlined below are three simple ways to manage the co-existence of NSX-T and NSX-v in your data centers with Tufin:

1. **Cleanup and optimize your policies so that the new and old data centers are not cluttered with unwanted and redundant rules**
2. **Deploy security policies in phases so that rollback can be ensured in the cases if disruptions and all the activities can be audited appropriately.**
3. **Achieve greater visibility and compliance to both the data centers through unified security policy**

Simplifies SDN migration

When an organization is building a software-defined network, it is usually not starting from the scratch. There is an existing data center and applications that need to be migrated to the SDN, and the organization needs to make this migration without disrupting business continuity, breaking compliance or introducing new risk to the organization. The Tufin Orchestration Suite meets all of these migration needs. Tufin automates the process of discovering all the applications in a data center and their connections. This information is critical as the team begins migrating servers and applications to a new SDN. Tufin's application modeling capabilities allow an organization to define and maintain dependencies between applications and services in order to understand how changing one application server affects other applications. This is especially important in a migration scenario where moving an application server to a new platform can have far-reaching ramifications. The migration team can model the application move to identify the impact it will have before making the change, and then Tufin can automatically provision the network to automate the change. Tufin can change the network configuration so that as physical servers are made into virtual machines, any connectivity requirements they had before will continue to work when they move into the new virtual environment. What's more, Tufin can identify the traffic used by an application and the existing legacy firewall rules which enable it, so that the security administrator knows how to build the proper network segmentation policy.
These capabilities enable the migration team to plan for and take the necessary actions while reducing the risk of overlooked dependencies.

© Copyright 2020 Tufin. All rights reserved.

Conclusion

As the market leading platform for the software-defined network, VMware NSX is redefining data center operations. Of particular importance is the ability to vastly improve network security by implementing security as close as possible to the application servers and data assets, they are intended to protect. Thus, the new data center is likely comprised of virtualized firewalls from VMware (i.e., the NSX distributed firewall); virtualized firewalls and other security devices from third-party solution providers; and the traditional physical components.

The Tufin Orchestration Suite provides single pane visibility and management of disparate and heterogeneous components that co-exist in one data center. This provides a unified and consistent approach to policy management across the enterprise network. The suite manages network segmentation; supports policy management and compliance; and eases the migration process to move into the SDN. The Tufin Orchestration Suite is an important solution to enabling the range of security capabilities of the software-defined data center.

About Tufin

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 Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. With over 2,000 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.

© Copyright © 2020 Tufin

Tufin, Unified Security Policy, Tufin Orchestration Suite and the Tufin logo are trademarks of Tufin.
All other product names mentioned herein are trademarks or registered trademarks of their respective owners.