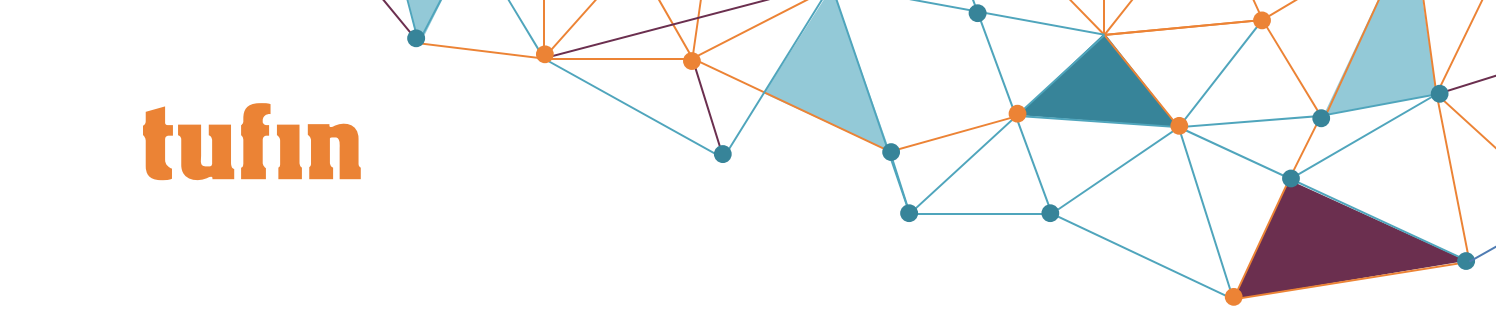


tufin

Operationalizing NSX Micro-segmentation in the Software-Defined Data Center

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

www.tufin.com

Introduction

The software-defined data center (SDDC) is redefining data center operations once again. SDDC is defined by three pillars: compute virtualization, storage virtualization and network virtualization. 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 containerizing 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.

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. With the networking piece of the puzzle solved, SDDCs will have a tremendous impact on how enterprises operate their data centers.

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 SDDC, 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™. It solves the fundamental challenge of network security, which 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 offers security by default, allowing network and security isolation, segmentation, and micro-segmentation with dynamic insertion of advanced security services.

The Tufin Orchestration Suite™ provides the necessary extension to the micro-segmentation capabilities enabled by VMware NSX. This unifies security policy management across not only the virtual networks within the software-defined data center 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 micro-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 SDDC 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.

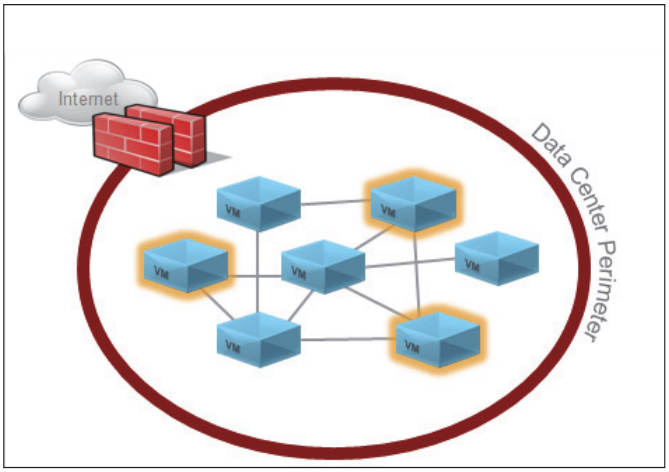


Figure 1: Network security at the perimeter

Courtesy of VMware®

Traffic moving within the data center is usually not inspected, which means that from one server – physical or virtual – to another within the VM, it's pos ny security checks. The problem here is that if one server gets inf 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. This latter scenario has been found to be the situation for numerous high-profile data breaches where the attacker has been able to move freely from one server to another in search of coveted data.

Of course it's possible to route traffic from a VM back through the perimeter firewall to have it inspected before sending it back inside to the data center. This works, but it creates a need to have higher capacity devices for the perimeter firewall because it now has to inspect more traffic as it looks at packets from within the data center as well as packets coming in from the outside. The traffic being routed in this unusual way creates an operational challenge because the network topology to make it work has to be more complex. Moreover, this approach simply isn't scalable.

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.

The solution to this problem, according to VMware, is micro-segmentation, which is illustrated in Figure 2. Instead of having just one firewall located at the perimeter, every VM within the data center is protected with its own firewall which runs the entire set of security

capabilities for any traffic going through the firewall. Traffic that goes from one VM to another doesn't have to be diverted to the perimeter firewall for inspection to ensure that everything does get inspected. From a security perspective this is a great model, but it is only feasible through the technology of a software-defined data center. This model of placing individual firewalls at every server is impractical in a physical data center because of the amount of firewalls that would be required and the complex routing instructions. An additional problem in this model is that traffic must be hair-pinned. In aggregate this approach would be an operational nightmare, not to mention cost-prohibitive.

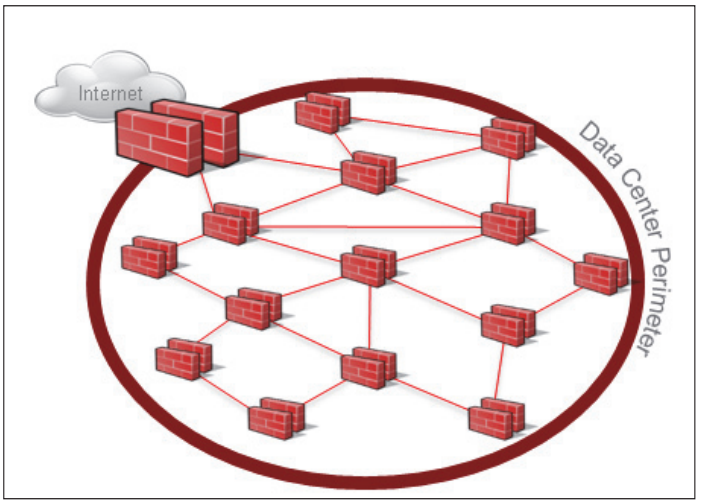


Figure 2: Network security via micro-segmentation

Courtesy of VMware®

Micro-segmentation provides numerous benefits. It allows granular controls and reduces the attack surface. It allows security administrators to see "east-west" traffic going between the VMs, previously not visible . It blocks harmful lateral movement within the virtual environment so that if one device is compromised in some way, the attack stops with that device and doesn't move on to others. In short, micro-segmentation enables a Zero Trust Model in which every piece of traffic that traverses the data center is inspected, regardless of where it came from.

There are multiple use cases for micro-segmentation. In the most basic sense, it can be used to isolate different environments; for example, to completely 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.

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 firewall or a more advanced firewall provided by a third-party partner such as Palo Alto Networks. Additional security controls can be plugged into the advanced segmentation scenario as well, such as IPS, 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.

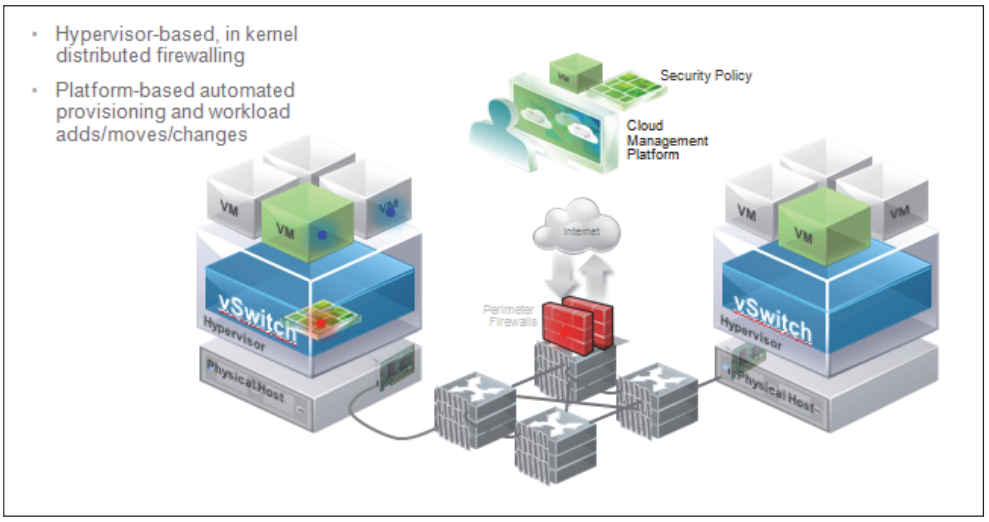


Figure 3: Security policy runs within the hypervisor level

courtesy of VMware®

The NSX platform can incorporate third-party products and make them part of the security infrastructure as well. NSX implements the concept of "traffic steering" to enable third-party firewalls to participate in the NSX inspection process. Figure 4 shows an example of traffic steering that utilizes a third-party Palo Alto Networks firewall.

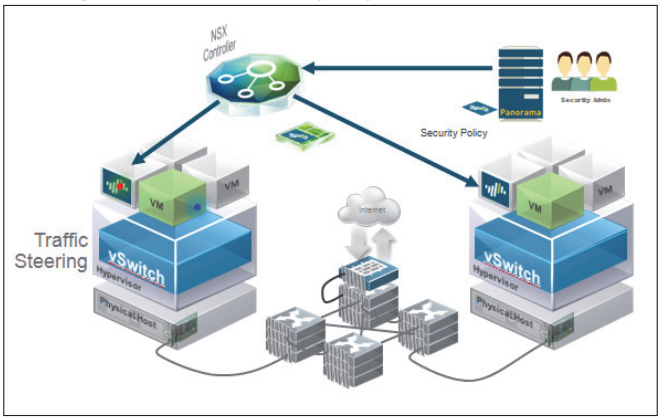


Figure 4: Traffic steering utilizing multiple virtual firewalls

courtesy of VMware®

In this example, the administrator defines a connection between the NSX controller and Panorama, the centralized management system for Palo Alto Networks devices. Panorama brings up a next-generation firewall (NGFW) that runs off a NIC on the physical host of the virtualized environment. The result is a Palo Alto Networks firewall within the VMware environment that has the same security policy as the physical Palo Alto firewalls running on physical devices within the data center.

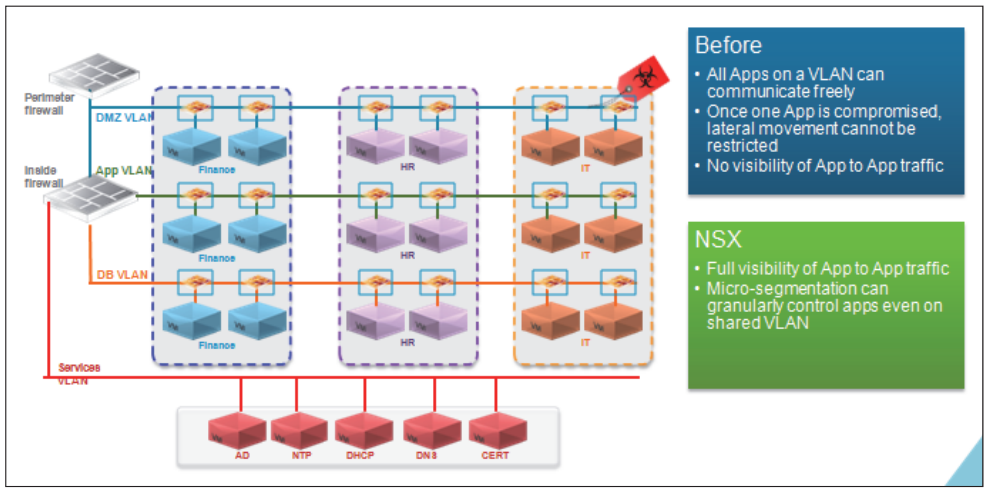
When a VM sends traffic and it hits the hypervisor, this traffic is first inspected by the NSX firewall and then the traffic is steered to the Palo Alto Networks firewall for additional security screening. It's possible to connect different types of security devices and policies, one after another, to create layered security. This service chaining capability is a significant feature of VMware NSX.

Here's one more common use case for micro-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 micro-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 actually 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.

Considering SDDC?

Evaluate:

- How can we maintain visibility and control across such 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?



courtesy of VMware®

Figure 5: Micro-segmentation to protect VLANs

In the Target Corporation breach as well as others that happened recently in the United States, the attackers used a vulnerable device and then from that device started going around the network in lateral movements, jumping from one network to the next until they reached the critical asset to which they wanted to gain access. Using micro-segmentation would actually block that from happening because each VM is completely inspected, minimally, 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 Data Center

Enterprise environments are heterogeneous with the SDDC 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 NSX distributed firewall); virtualized firewalls and other security devices from third-party vendors like Palo Alto Networks, Check Point and Intel Security; and the traditional physical components such as Cisco, Juniper Networks and F5 Networks.

There are several main security management technologies pertaining to the SDDC: micro-segmentation, policy management and compliance, and migration to the SDDC.

Visibility and management of micro-segmentation

Organizations need to be able to manage micro-segmentation both inside and outside the NSX environment. Micro-segmentation provides better security by tightening the security controls around a server (virtual machine) when compared to traditional security controls, which are based on subnet segmentation. Operationalizing micro-segmentation requires effective configuration and managed. How can I ensure that my NSX segmentation is properly configured to take advantage of this innovative technology? This includes not unnecessarily exposing servers when making changes, and ensuring that business applications have full connectivity at all times.

Managing policies and compliance

A second key area involves policy management 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 north-south traffic as well as 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 SDDC. The administrator needs to understand what security devices the

traffic is going to pass through and simulate what would happen if such traffic does indeed go through. This will help him understand if the traffic will be accepted or dropped even before he makes 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 Palo Alto Networks firewall that is running right after it using traffic steering. This is very hard to do, especially in an environment of service chaining where different sets of policies draw on different technologies and vendors' devices.

The Tufin Orchestration Suite Helps to Operationalize Micro-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.

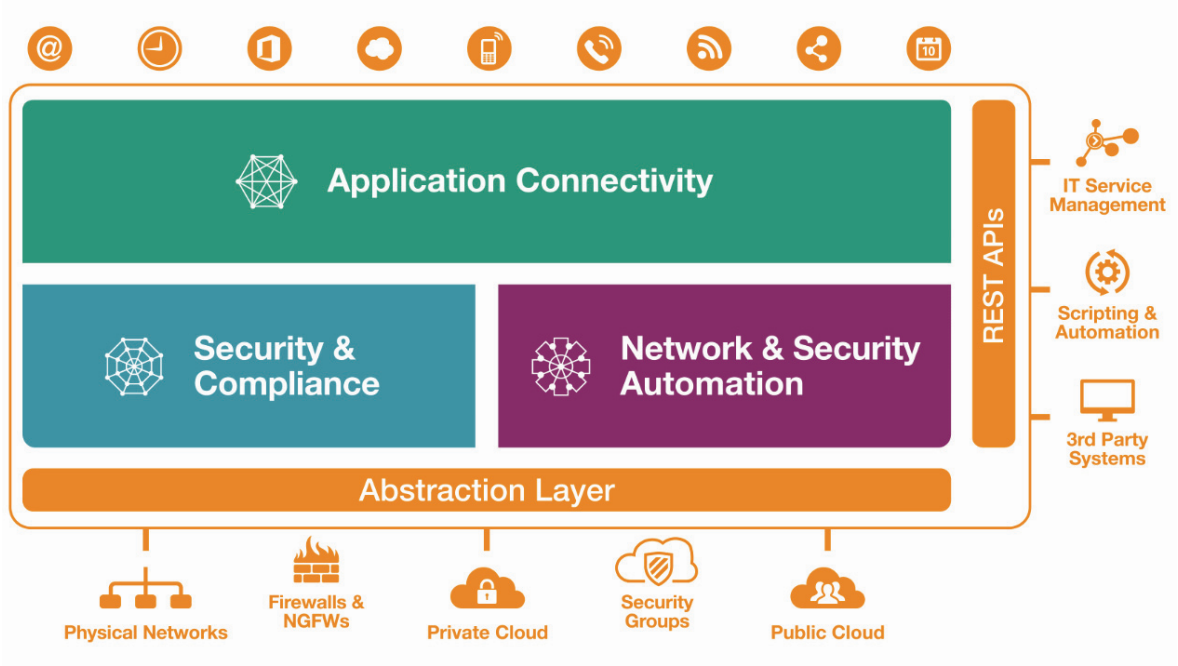


Figure 6: The architecture of the Tufin Orchestration Suite

Briefly, here's a description of what each of these components does.

- The ***Business Application & Services*** component allows an organization to model its business applications and services, defining the network resources they require in order to work.

- The ***Security & Compliance*** component holds the organization's Unified Security Policy. The USP defines the desired (or required) security policies that must be enforced in the organization. These include segmentation policies, best practices, regulatory compliance frameworks (such as PCI-DSS, NERC CIP, HIPPA, etc.) and any other security policies the organization wants to comply with internally.
- The ***Network & Security Automation*** component enables change automation in the network. This component performs the actual security automation activities, while checking with the *Security & Compliance* component that these automated changes are not breaking or violating the desired security and compliance policies.
- The ***Network Abstraction*** component hides the network complexities from the other components. It maps and holds the network topology and interacts with the different networking and network security technologies running in the network.

How the Tufin Orchestration Suite Works in SDDC 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.

Tufin manages micro-segmentation

There are three ways in which Tufin contributes to the management of micro-segmentation for the SDDC. First, Tufin provides a unified and consistent policy across both physical and virtual environments, with clear graphical visibility into that policy. Second, Tufin takes a centralized approach to identifying and managing violations and exceptions. And third, Tufin can automatically check any planned change against a segmentation policy before it is actually 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 axes, and the colors of the blocks signify what the permitted communication between those zones should be. 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. Of course a zone could span across physical, virtual or hybrid cloud platforms.

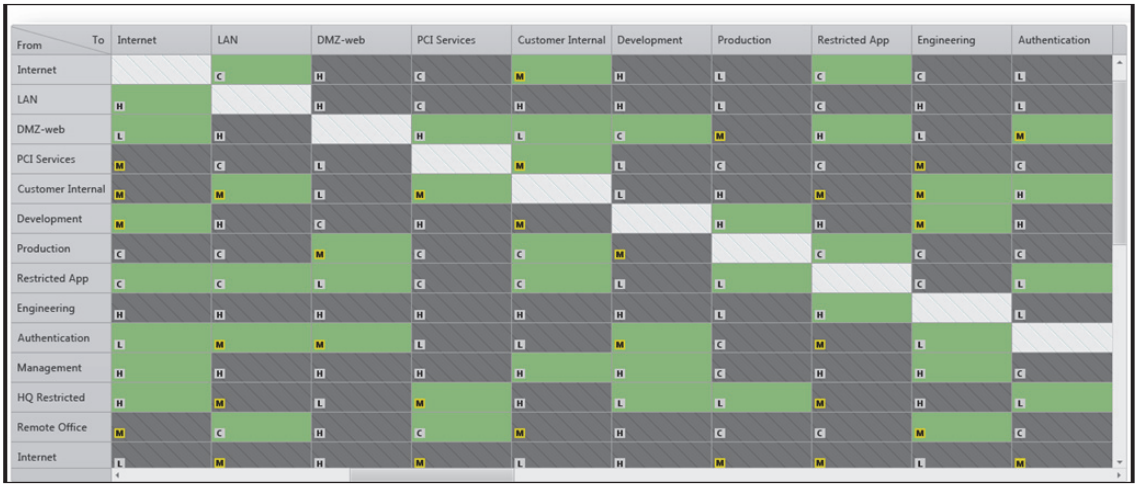


Figure 7: Tufin's micro-segmentation management matrix

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 actually 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.

Figure 8 shows a sample of a policy violation report.

#	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 needs occasionally require an exception to a desired segmentation policy; for example, to allow a specific business application access in order to run properly, 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 give them an expiration date so they will have to be re-examined or removed after a specific date. This gives the security administrator time to talk with the business application owner to find a way to either change how the application

works or change the segmentation policy. All policy exceptions are automatically documented and auditable.

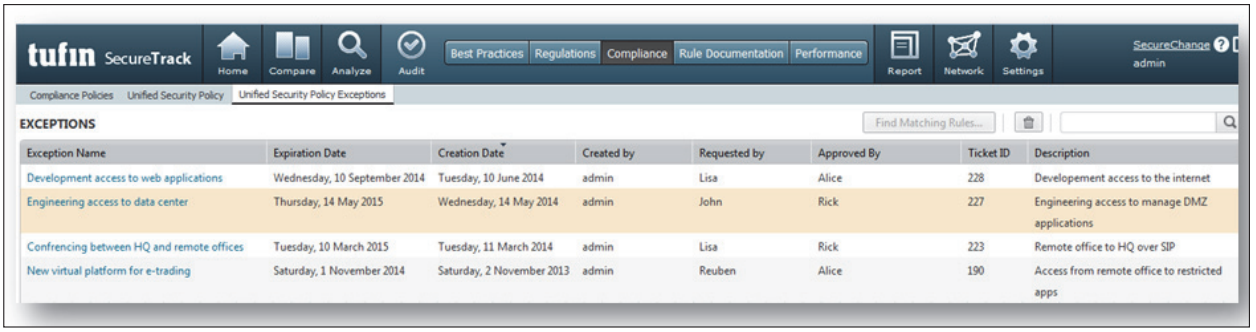


Figure 9: A sample exception report

The Unified Security Policy also proactively identifies potential violations of segmentation policy before the change is actually made. The administrator who is handling such a change request can decide either to add it as an exception or to go back to the person who requested the access to tell him it's not allowed because it violates the segmentation policy.

Tufin supports policy management and compliance

The Tufin Orchestration Suite supports policy management and compliance for the software-defined data center in a number of ways. Tufin offers centralized management for multi-vendor policies and technologies, and can assure continuous regulatory in an automated way. The Unified Security Policy provides all sorts of 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 full audit trail and documentation--so that all changes can be tracked and reports can be produced for auditors when necessary.

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.”

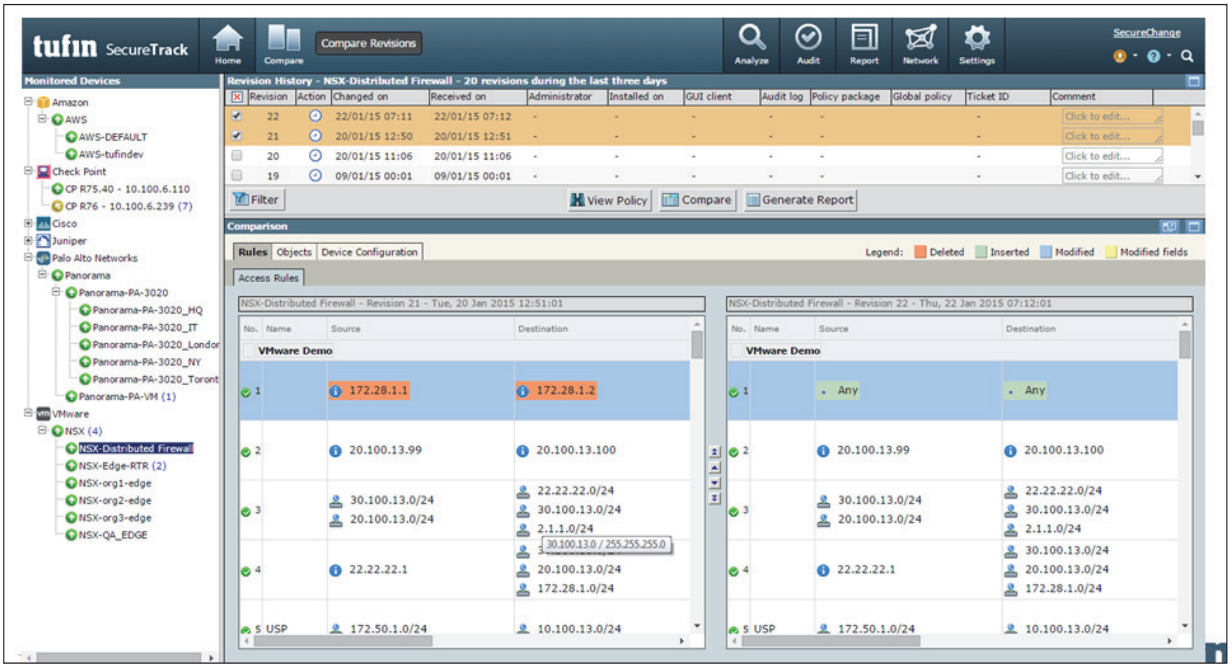


Figure 10: A "before" and "after" comparison of a policy change

There are overview and detailed violations reports for all sorts of compliance policies such as PCI, SOX and others. 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 actually 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. In a future enhancement, this feature will support traffic steering in the event that traffic would have to pass through multiple chained 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.

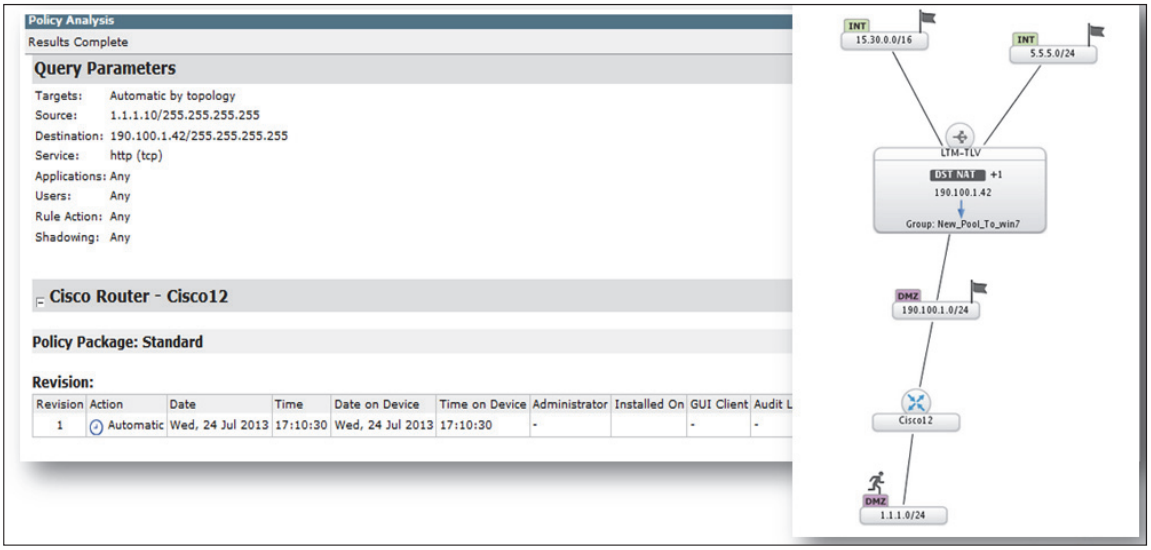


Figure 11: An example of "what-if" policy analysis

Tufin simplifies SDDC migration

When an organization is building a software-defined data center, it is not starting from scratch. There is an existing data center and existing applications that need to be migrated into the SDDC, and the organization needs to make this migration without disrupting business continuity, breaking compliance or introducing new risk to the organization. And the organization needs to do all this as efficiently as possible, in an automated fashion. 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 SDDC. 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 see what impact it will have before actually making the change, and then Tufin can automatically provision the network to accommodate this change if desired. 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 micro-segmentation policy. These capabilities enable the migration team to plan for and take the necessary actions while reducing the risk of overlooked dependencies. Moreover, this process can extend over both virtual and physical environments.

- For an in-depth look at how Tufin Orchestration Suite supports data center migrations, read Tame the Network and Security Challenges of a Data Center Migration.

Conclusion

As the market leading platform for the software-defined data center, VMware NSX is redefining data center operations. Of particular importance is the ability to vastly improve network security by implementing virtual security devices as close as possible to the application servers and data assets they are intended to protect. Third-party security devices from the likes of Palo Alto Networks, Check Point Software Technologies, Intel Security, Fortinet, Juniper Networks and other vendors also fit into this mix to fully enable micro-segmentation. 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 micro-segmentation; supports policy management and compliance; and eases the migration process to move into the SDDC. The Tufin Orchestration Suite is an important solution to enabling the range of security capabilities of the software-defined data center.

About Tufin

As the market leader of Security Policy Orchestration, Tufin automates and accelerates network configuration changes while maintaining security and compliance. Tufin's award-winning Orchestration Suite™ gives IT organizations the power and agility to automate and enforce security policies across complex, multi-vendor enterprise networks. With more than 1,500 customers worldwide, Tufin enables IT to implement network changes within minutes, with increased accuracy and security.

For more information about SecureChange, visit www.tufin.com.