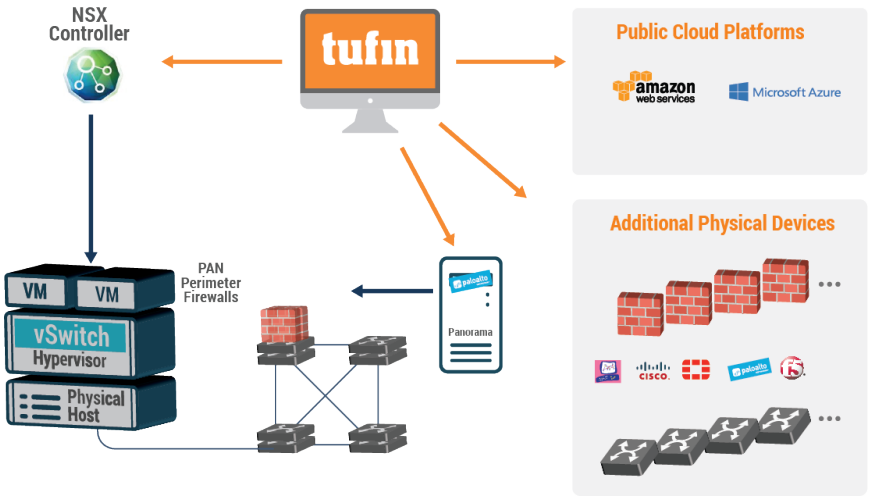
NSX Reference Design Document

Contents

Overview

VMware SDDC Approach Redefines Data Center Network Security

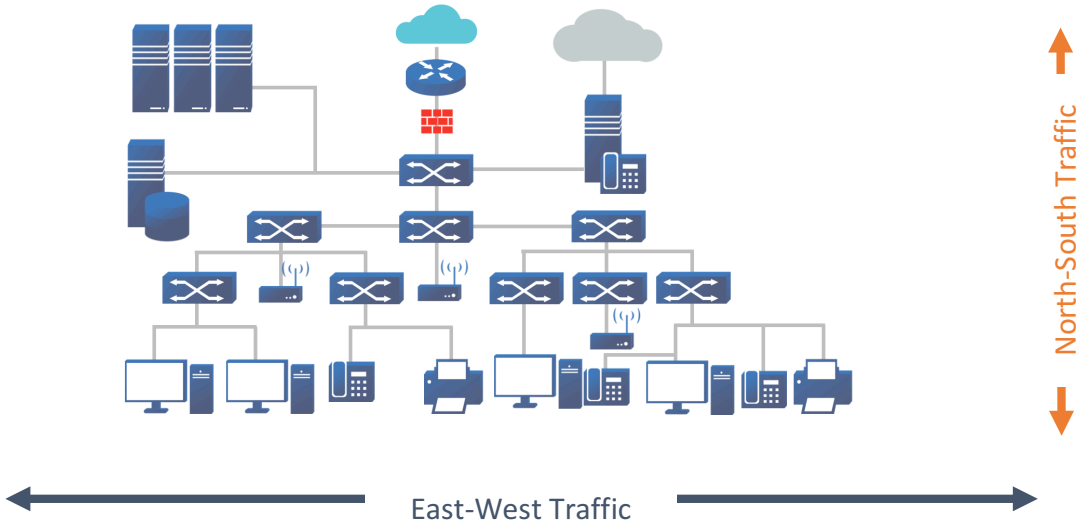
The Software-Defined Data Center (SDDC) enables a substantially improved operational model that provides greater speed and agility, lower operational overhead, and lower capital expenditure. VMware NSX delivers network virtualization for the SDDC, with a full service, programmable platform that provides 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 is achieved through security controls at the unit level or virtual machine level. Leveraging network virtualization



technology, the SDDC 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.

SDN and Securing East-West and North-South Traffic

East-west network traffic is the transfer of data packets from server to server within a data center in the same SDN (NSX) environment. North-South indicates network traffic from the NSX environment to the legacy datacenter or vice versa.

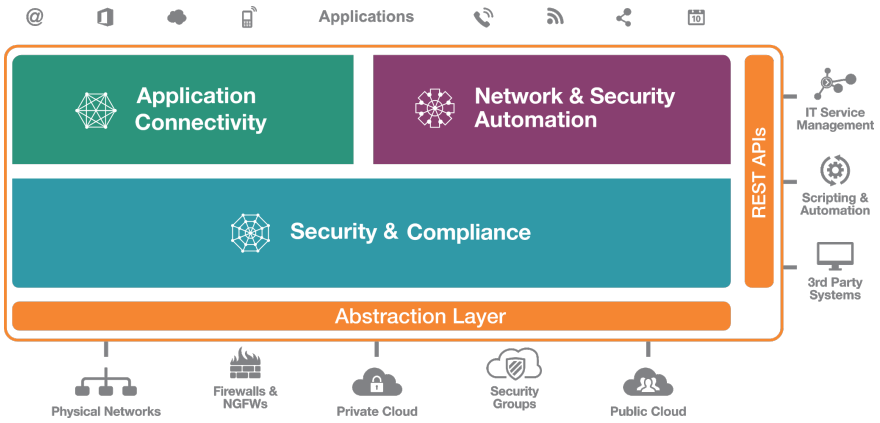


Visibility into both types of traffic – east-west and north-south – is critical for organizations to determine the best security practices for their networks and data centers. While many organizations focus on securing external traffic that enters their networks, it is increasingly important for organizations to monitor internal traffic patterns to identify malware that has infiltrated the network and for insider threats.

Micro-segmentation (greater detail in a following chapter) significantly reduces the attack surface available for malicious activity, and lessens the impact of an attack spread through east-west traffic. If the data center is segmented into logical units, data center administrators can tailor unique security policies and rules for each logical unit. This tightly-coupled approach eliminates the tedious, error-prone manual configuration processes that often lead to security flaws after a migration.

The Tufin Orchestration Suite™ Solution for VMware NSX

The Tufin Orchestration Suite™ is a complete solution for automatically designing, provisioning, analyzing and auditing network security policy 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 adherence and identify violations to security policy, and automate changes throughout the entire data-center via a single interface. The Tufin Orchestration Suite™ provides unprecedented visibility and control of security in the SDDC ensuring a unified security policy management across the entire enterprise – including physical and virtual networks as well as hybrid cloud platforms.



There are four use cases for the integration points between Tufin Orchestration Suite and VMWare NSX:

1. **Visibility** – View and track changes to security policy and configuration in the NSX environment.
2. **Micro-segmentation** – define and manage micro-segmentation both within the NSX environment as well as with the external Data center.
3. **Policy-driven change automation** – automate changes through Tufin SecureChange while ensuring adherence to corporate security policy, understand the potential risk, and push changes to the relevant devices in NSX and the DFW, and outside of it to the appropriate FWs.
4. **Integrated policy-driven change automation** – automate changes through integration with VMWare vRealize Orchestrator (vRO).

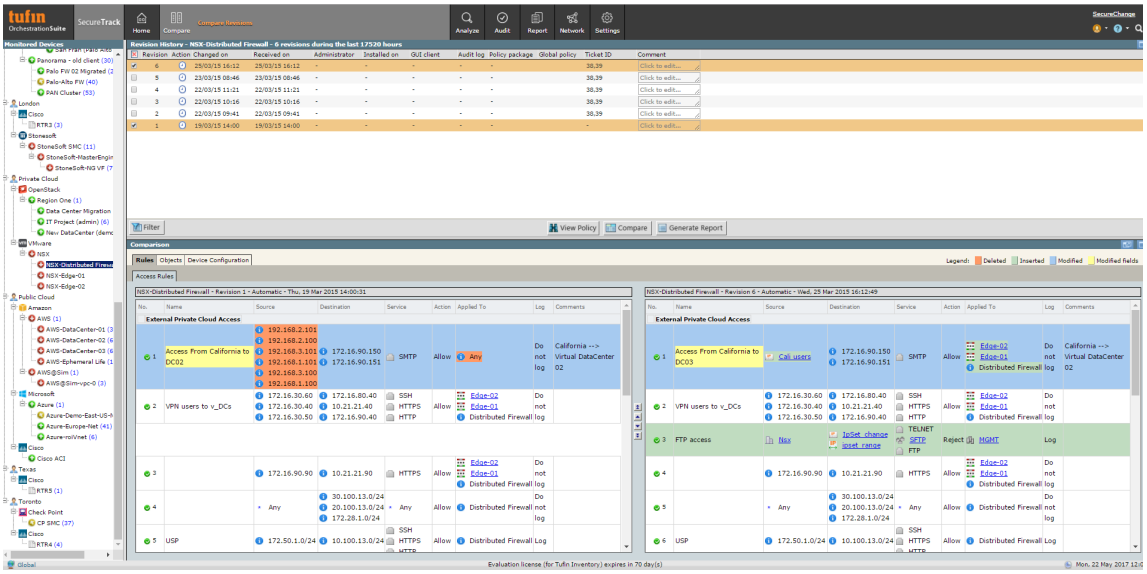
The following chapters cover the above use cases in depth while outlining the business challenges and how Tufin can help solve them.

Visibility and SDN – You can't secure what you can't see

Challenge:
When it comes to security policy management, organizations need to manage their policies centrally—even though the policies may be enforced on different platforms from different vendors on physical, virtual, and cloud-based platforms. Security managers need broad and unified visibility, an audit trail of all changes, and advanced analysis and reporting capabilities.

Configuration of security rules must be applied to the Distributed Firewall (DFW) within NSX, NGFWs, and on legacy firewall (e.g. Check Point, Palo Alto, Cisco, Fortinet) to ensure connectivity and security. Security managers require visibility into changes across all of these firewalls – what was changed and who changed it – without jumping between different tools or different dashboards. This becomes a necessity as enterprises networks become more complex with a greater number of security devices installed.

Tufin Solution:
The Tufin Orchestration Suite™ serves as a single pane of glass to manage and control security across hybrid cloud and physical networks. The Suite provides security managers with the same level of visibility and control in their new software-defined environment that they are accustomed to in a traditional data center.
In addition, the Tufin Orchestration Suite™ retains an accurate audit trail of all changes and uses advanced change monitoring and analysis for full accountability. All changes can be tracked and reports can be produced for auditors when necessary. The screenshot below demonstrates change tracking of a security policy, ensuring that at any point it's easy to see who did what, when and why, and this can be fully documented for future reference.

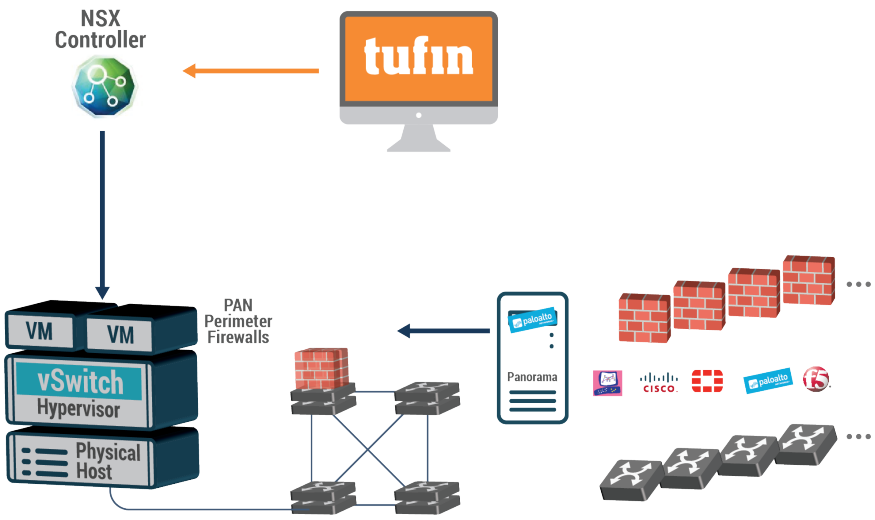


Tufin's SecureTrack provides a side-by-side comparison of the policy before and after changes.

Managing Micro-segmentation

Challenge:
Organizations need to be able to design and effectively 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) than traditional security controls based on subnet segmentation. Operationalizing micro-segmentation requires effective configuration and management. However, approaching the challenge often leads with "How can I ensure that my NSX segmentation is properly configured to take advantage of this innovative technology, that servers are not inadvertently exposed, and that application connectivity is retained?"

Managing microsegmentation in a complex environment is difficult. A key parameter is to be able to track and manage this complex process in a simple, visualized way without manually applying different security configurations and rules across NSX and the rest of your firewall devices.



Tufin Solution:
There are three ways in which the Tufin Orchestration Suite™ enables successful management of micro-segmentation for NSX. The Tufin Orchestration Suite™ provides:

- A unified and consistent policy across both physical and virtual environments, with clear graphical visibility into that policy.
- A centralized approach to identifying and managing violations and exceptions.
- Automatic checks of planned changes against a security policy before it is implemented to make sure that the change is not introducing a new policy violation.

The figure on the following page shows the Tufin Orchestration Suite's™ zone segmentation matrix which is an element of the Unified Security Policy (USP). This matrix represents the different network zones on both the horizontal and vertical axes, and the colors of the blocks indicate the permitted communication between the two intersecting zones should be. In the zone segmentation matrix, a green block represents that traffic of specific services between two zones is allowed, a gray block means that traffic is not allowed, and a red block indicates traffic is allowed which currently violates security policy. Each zone represents physical, virtual or hybrid cloud platforms.

From \ To	Amsterdam_Ext	Amsterdam_SiteA	Amsterdam_SiteB	Cali_bckp-site	London	p_DataCenter	p_PM	p_RnD	p_Sales
Amsterdam_Ext		H	H	H	L	H	H	L	H
Amsterdam_SiteA	H		H	H	H	H	H	L	M
Amsterdam_SiteB	H	H		H	H	H	H	M	H
Cali_bckp-site	H	H	H		H	H	H	H	H
London	H	H	H	H		H	H	H	H
p_DataCenter	H	H	L	H	H		L	L	L
p_PM	H	H	H	H	H	H	H	L	L
p_RnD	H	H	H	H	H	H	H		L
p_Sales	H	C	M	H	H	C	H	L	
TexasVPN users	H	H	C	H	H	H	C	H	H
Toronto	H	H	H	H	H	H	H	M	L
Virtual_DC-01	H	H	H	H	H	H	H	H	H
Virtual_DC-02	H	H	H	H	M	H	H	H	H
Virtual_DC-03	H	H	H	H	H	H	H	H	H
Virtual_DC-04	H	H	H	H	H	H	H	M	M

The Tufin Orchestration Suite™ zone segmentation matrix

In the NSX environment zones can be IPs or subnets, but are most often Security Groups given the dynamic nature of the SDDC. As VMs are provisioned and destroyed rapidly, the usage of IPs less relevant due to unmanageability.

Once an organization has designed its segmentation policy and implemented it to produce the visual matrix view, the Tufin Orchestration Suite™ analyzes the network to identify the gaps between the desired state of security policy compliance and the actual enforcement policies running across network firewalls, routers, and security groups. Unlike manual spreadsheets that security administrators often create and rely on, this matrix is connected to the network and automatically detects and alerts firewall administrators of violations. For NSX, this ensures that if a rule is added to the DFW or to the perimeter FW, the impact on the relevant zones is known.

Operational needs occasionally require an exception to a desired segmentation policy. For example, allowing a specific business application non-compliant or risky access may be required in order to run properly, even though it introduces risk to the organization. The Unified Security Policy provides centralized exception management that allows a security administrator to identify and manage exceptions, assign an expiration date to non-compliant rules, and ensure that they are re-examined and approved, or removed, by a specific date. This process provides the security administrator time to talk with the business application owner and find a way to either change how the application works, or change the segmentation policy. All policy exceptions are automatically documented and auditable.

Automation through the Tufin Orchestration Suite™

Challenge:

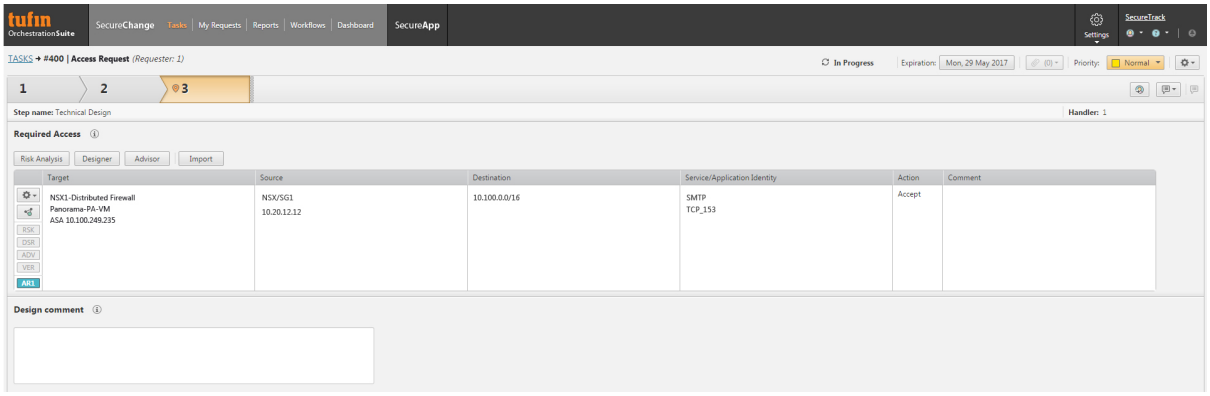
NGFWs, such as NSX DFW, and legacy firewalls are the first line of defense, but effective management of firewalls drains personnel resources from security programs already coping with a shortage of skilled labor. Regardless, security policies need to be checked, firewalls optimized, and continuous compliance and demonstrably achieved. These firewall management tasks are typically manual processes that are both time consuming and rife with manual error, necessitating a solution to eliminate misconfigurations and return personnel resources to strategic or imminent challenges.

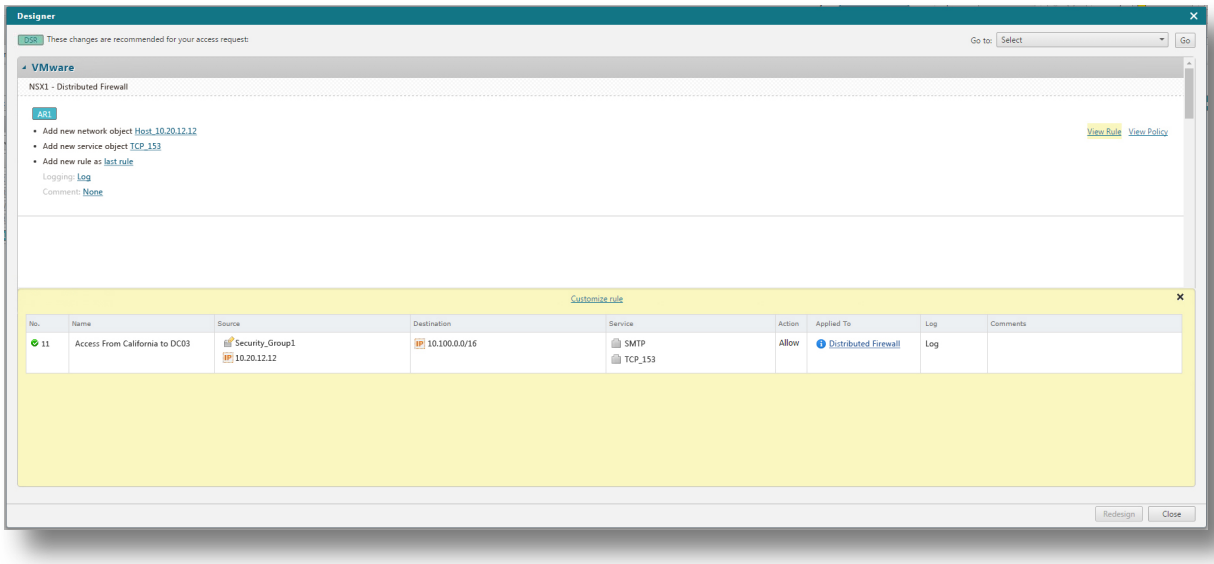
Workloads can run dedicated on SDN environment or span across NSX and on-premise infrastructure, hence automation must support the multiple platform and technologies used. Failing to support the diversity of vendors beyond NSX prohibits achieving agility, and delays access to a data center's database when behind different firewalls and routers, and the tasks associated with managing all of them.

Tufin Solution:
The Tufin Orchestration Suite™ provides central management and a fully automated change process, providing end-to-end connectivity across the hybrid network while meeting security policy mandates. End-to-end automation of network security changes with baked-in security and compliance enables both North-South and East-West connectivity by provisioning to the NSX Distributed Firewall as well as legacy firewalls using Security Groups.

The change process provided by the Tufin Orchestration Suite™ includes automated risk analysis for built-in policy compliance and best practices, automated design and provisioning for on-prem firewalls and NSX, and automated connectivity verification to boost productivity and accelerate delivery. Tufin delivers automated provisioning for changes to NSX security groups (or IP and IP sets) and guides users to ensure that the right security groups are changed. The automated change design is based on the most accurate topology simulation and efficient path analysis across NSX and other platforms/vendors

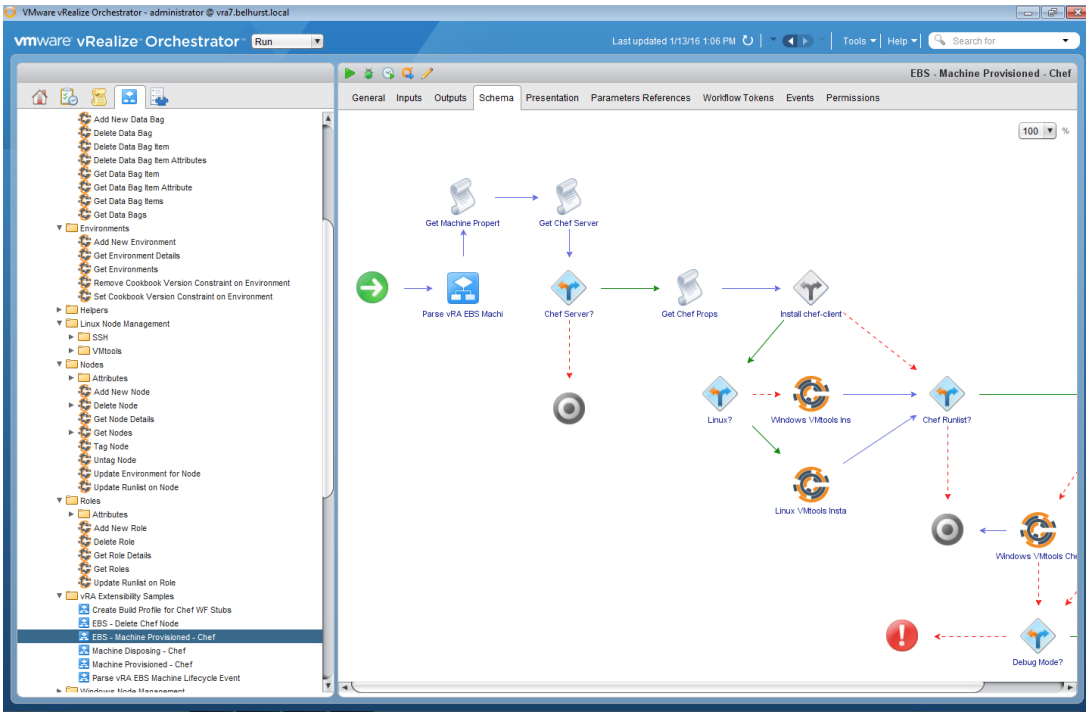
While all these capabilities are supported through the SecureChange UI, customers often integrate Tufin workflows and process management into their existing third-party ticketing tools (e.g. ServiceNow or Remedy) through APIs or integration applications to keep their existing business processes and flows unchanged.





Automation through integration with VMWare vRealize Automation (vRA)

NSX and vRealize Automation are two major products from VMware. vRealize Automation can build a private cloud environment while NSX builds the underlying software defined network. Both the efficiency and security control over the SDDC is realized when using NSX and vRealize Automation in concert. With NSX you can build dynamic routing, load balancing, firewall rules to create the virtualized network – vRealize Automation uses vRealize Orchestrator (vRO) as its underlying orchestration engine.



Integrating vRO with SecureChange enables customers to achieve full automation for designing and provisioning application connectivity. Together, vRA and vRO can be used to spin up a multi-layer application through a single click along with its network, firewall rules, and load balancer.

Applications running within the SDDC and consuming non-SDDC resources (e.g. LDAP server or DB), require north-south connectivity. This can be achieved by incorporating vRO workflow calls to a Tufin workflow through APIs for:

1. **Topology Discovery**: find traditional firewalls in front of the provisioned VMs.
2. **Risk Analysis**: Compliance check against Tufin USP before implementation.
3. **Provisioning**: Pushing changes to traditional firewalls in front of the provisioned VMs running on NSX.

A typical flow can be:

1. Deploy new VMs from vRO workflow based on VM templates (using vCenter API to provision new VMs).
2. Cache VMs network information like IP Allocated, and Policy Template
3. Use the HTTP-REST Client from vRO to open a ticket on SecureChange (JSON formatted query)
4. In SecureChange, run a fully automated workflow for provisioning rules on Cisco ASA and Check Point firewalls and connect the VMs to the network.

The above is similar to other ITSM integration like BMC Remedy, ServiceNow, and other tools (further available in the Tufin Professional Services Catalogue).

Conclusion – Integration Key Benefits

The integrated VMware NSX™ and Tufin Orchestration Suite™ solution delivers visibility, unified security policy management, and compliance across physical and virtual networks, and hybrid cloud. The strategic integration enables IT organizations and security teams to:

- View and manage security policies across the network from a single pain of glass, thereby reducing complexity.
- Track changes to security policies on NSX as well as on other leading cloud platforms, and present what was the change and who did it.
- Reduce audit preparation time and enable continuous compliance using the Unified Security Policy
- Design, implement, manage, and monitor micro-segmentation across NSX, physical and hybrid networks
- Visualize policies and network connectivity across the heterogeneous corporate network, enabling IT teams to troubleshoot connectivity issues quickly and easily
- Maximize agility with end-to-end automation of network security changes with baked-in security and compliance providing:
    - Automated risk analysis for baked-in security and compliance
    - Automated change design based on accurate topology simulation and path analysis across NSX and other vendor's platforms
    - Automated provisioning for NSX to reduce complexity, eliminate human error, and ensure connectivity