A Primer on Network Service Orchestration

anuta networks

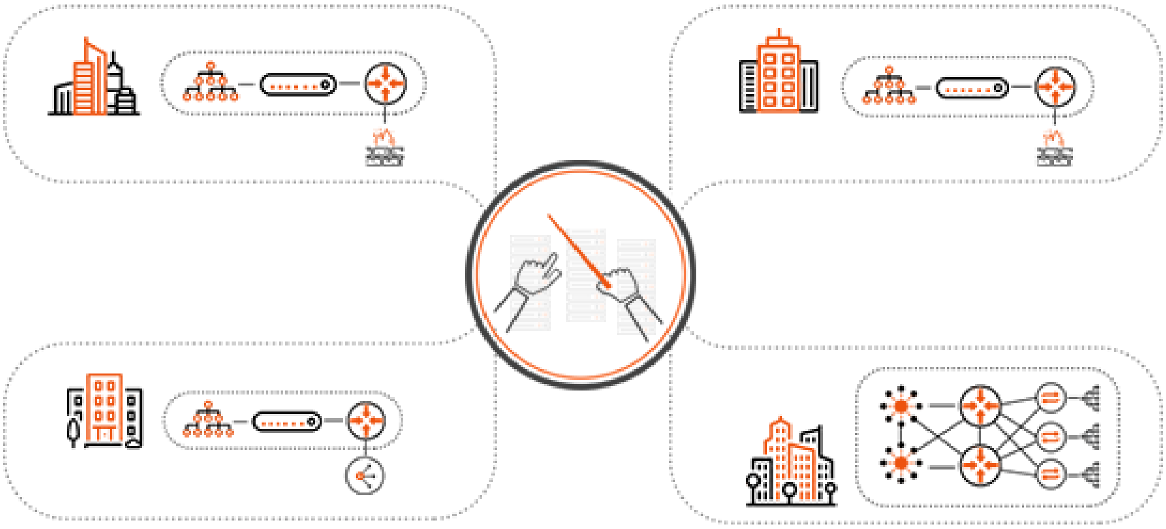
Contents

What Is Network Service Orchestration?

Network Service Orchestration or NSO, commonly refers to a software solution that helps network operators configure and automate multiple network elements as per a given service definition and workflow.

NSO allows processes that traditionally entail many manual steps to be conducted end-to-end with the push of a single button, even by non-technical staff.

> *NSO is an application that can take a request from a customer via a web portal for new virtual server requiring provisioning.*
>
> *This ideal app will analyze the network configuration and implement the configuration change for the customer and then update the billing system. The network itself might implement in the physical network, in a virtual overlay on hypervisors, across the WAN via encrypted tunnel or one of many other options. The connectivity is far less important than the orchestrated service establishment across many devices and platforms.*
>
> **- Greg Ferro**



Some examples of a network service include configuring L2 and L3 VPNs, On-boarding remote branch office equipment using zero-touch provisioning, configuring Security and QoS policies for

3-Tier applications in Data Center, Configuring Bandwidth control and Application routing policies in a remote branch, Interconnecting multiple public, and private clouds, etc.

A network service typically spans multiple network elements such as routers, firewalls, load-balancers, VPN gateways, WAN optimizers, Web Security Services. These elements can be physical or virtual appliances and often sourced from different vendors (E.g., Arista, Brocade, Cisco, Checkpoint, Citrix, F5, Fortinet, Juniper, Huawei, Riverbed, Palo Alto Networks, VMware, etc.).
The network elements may reside in an enterprise Data Center (also known as Private Cloud), a Remote Branch office, a Service Provider backbone network or in public cloud (such as AWS VPC).

Why Network Service Orchestration?

Traditional Network Management software is not able to keep up with the demands on the network operators. Every year, the underlying hardware keeps evolving (e.g., Fabric path, SDN controllers), the number of networking vendors increase, and the communication methods (E.g., CLI, API, SNMP, NETCONF) keep changing. In many companies, the developer who wrote the expect or TCL scripts left the company and every simple change becomes a new project. Ultimately, network operators are resorting to spreadsheets to maintain VLAN numbers, router credentials, etc. The manual configurations are time-consuming, expensive and difficult to scale and maintain. The vendor specific EMS/NMS software is expensive and necessitates vendor lock-in. Because of these reasons, Network roll-outs take 6+ months.

In contrast, a NSO uses the concept of abstraction to capture network configuration, operational data and policy in a vendor-neutral format and integrates with self-service portals. The network architects customize built-in service models, and Orchestrator will take care of the differences in underlying infrastructure. As a result, the network operators don't have to learn complex CLIs from multiple vendors and network services can be rolled out within minutes.
For example, let's say the operator has to create a VLAN for a specific application. In the traditional approach, the operator has to login to every router and configure using CLI or GUI. On the other hand, a NSO automatically discovers the network topology and all the dependencies for creating a VLAN. It auto-generates the CLI or API calls for each vendor device and executes an atomic transaction across all devices.

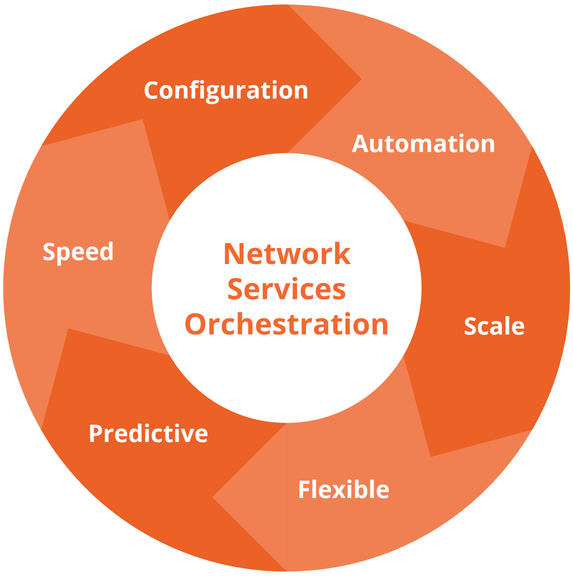
Automation vs. Orchestration

> *Enabling an interface? Automation.*
> *Configuring a VLAN on a switch? Automation.*
> *Creating interface descriptions based on LLDP neighbors? Automation.*
> *Creating a VLAN service by enabling edge interfaces, configuring access VLANs, creating VLAN-to-VXLAN mappings, and testing the end-to-end connectivity? Orchestration.*
> *Put simply, "Network Automation = Squeezing Grapes" and "Network Service Orchestration = Making wine."*
>
> **- Ivan Pepelnjak**

What are the business benefits of Network Service Orchestration?

NSO avoids technology and vendor lock-in for investment protection. It allows easy integration and automation with customers' self-service portals, 3rd party web-applications, and OSS/BSS via REST APIs and has no hard-coded parameters for the rollout of new device types and new services.

Customers can Realize immediate ROI through a low-risk approach. Initially, NSO can run side-by-side with the existing EMS/NMS solutions or replace them if needed. On average, NSO has a payback period of 6 months.



NSO helps customers increase revenue by quicker time-to-market. By designing and deploying new services so much faster, time-to-market is reduced from months to a few hours. New device types previously unknown to the system are rolled out in 15 minutes via configurable MIB polling policies and rules. Moreover, automated services of predefined custom-designed service templates are provisioned via GUI or REST API to maximize network agility and programmability.

NSOs lowers OpEx and CapEx. It dramatically improves cost structure through complete vendor independence and automation of key processes of purpose-built multi-vendor networks based on customized hardware and silicon via full REST API to unify traditional network management and open, SDN-style network programmability and Service Lifecycle Orchestration.

NSO reduces the overall complexity of the network by eliminating operational silos and unifies all management functions across end-to-end, multi-vendor and multi-layer networks into a single-pane-of-glass platform.

Where is the Network Service Orchestration ROI?

A recent McKinsey study revealed that more than $60B is spent on Network Operations Labor and Tools annually.

75%

of OpEx is spent on network changes and troubleshooting.

90%

of the network changes are performed manually

70%

of Policy violations occur due to human error

NSO reduces OpEx, avoids human errors, eliminates outages and introduces consistency.

The NSO ROI is achieved in three main benefits.

Productivity

Labor increases per person

Quality

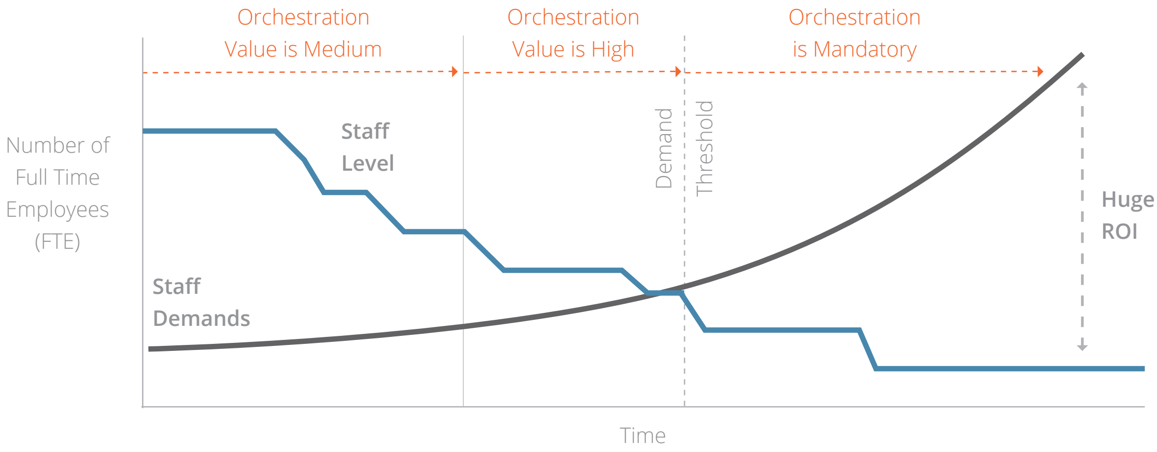
Decline in errors

Adaptability

Reduction in time to provision new services

Productivity

NSO enables Operators to do more with less.



Initially, the ROI on NSO will appear low as it requires extra investment in staff to develop the workflows and service models. However, as the deployment grows and the demand for services increases, the ROI will improve. When NSO is implemented successfully, the required staff level shrinks even as the demand for services increases. The ROI is so compelling that beyond a demand threshold, NSO becomes mandatory.

The cost savings such as labor reduction, reduced cost of errors and top-line revenue effects are easy to quantify. But there are other potent soft benefits such as brand reputation, agility, competitive differentiation and flexibility to pursue new opportunities.

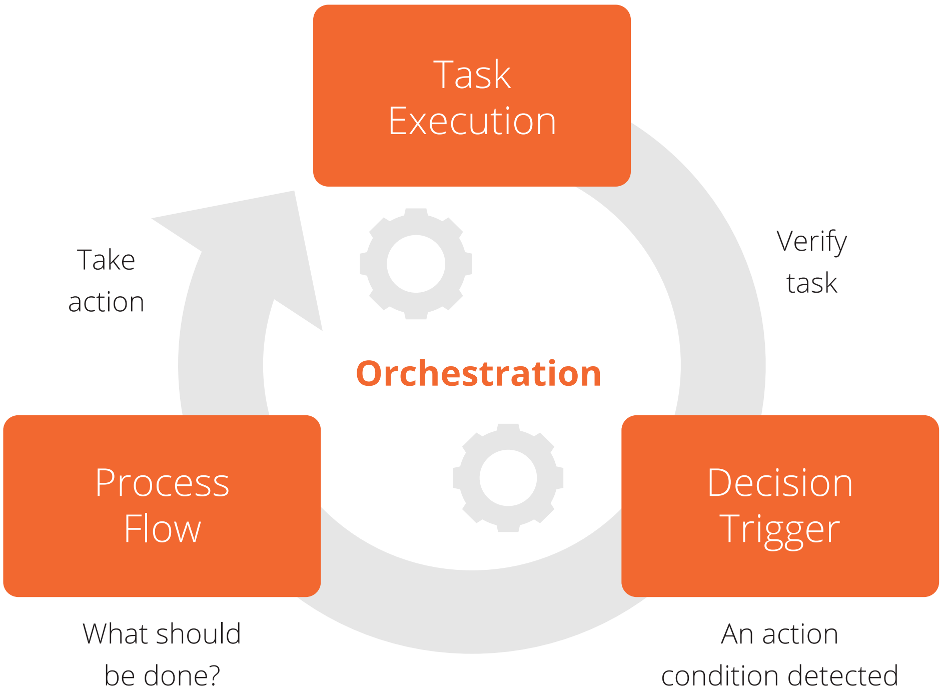
Quality

NSO introduces consistency that automatically improves quality. Quality leads to good reputation and more business.

Many Customers witnessed dramatic improvements in metrics such as the number of outages, mean time to repair and the staff required to troubleshoot the outages.

Adaptability

NSO checks on conditions and acts based on policies. The Service will be adapted to changing demands yielding a quicker time to market and better quality. Ultimately, the system becomes nimbler to introduce new services.



NSO formalizes the closed-loop behavior within all aspects of network operations. Each action will be validated and documented to fine tune the decision process. The software detects every change in the infrastructure and offloads the operators by automating some of the decisions in real-time. With higher predictability, the network team can embrace newer challenges to support changing business demands.

What is the Network Service Orchestration Lifecycle?

Network Service Orchestration coupled with real-time Telemetry automates Service Assurance in a closed-loop system. With NSO, Network Architects can deploy a predictive and proactive system that generates insights for Application, Client, and Compliance to isolate cause in few clicks.

Plan

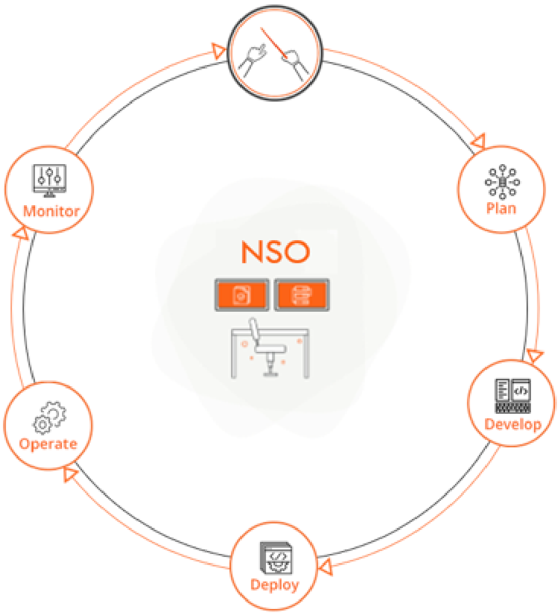
During the planning phase, Network admin collects standardized configurations for existing or planned services. The information could be a simple text file with CLI commands or sample API calls with parameters.

Product Managers and Network architects can describe the service they want to offer on their infrastructure. They can use built-in Service Models (starter kits) to describe various network services such as L2 VPN, L3 VPN, IWAN, App Delivery, etc. NSO also provides service model framework using which you can extend these starter kits with SLAs.

Develop

DevOps teams can take the starter kits, introduce business logic, workflow and integrate with 3rd party software in the infrastructure and define SLA metrics as part of the service template. NSO also provides a normalized network model. The developers don't need to know the semantics of individual vendor devices. NSO simplifies the task for devops team, so they can develop common code base that works for multiple deployments. NSO provides development toolkits, code generators to automate most of this task. DevOps can customize for various vendors and use-cases, introduce versioning, release management to infrastructure using YANG models.

Network Service Orchestration and Assurance



Plan
Gather Service Requirements

Develop
Develop & Test Service Models using SDK

Deploy
Deploy & Maintain Network Services

Operate
Greenfield/Brownfield Services

Monitor
Monitor Services & Remediate

Deploy

The services are advertised in a self-service catalog or OSS/BSS using the REST API. When someone orders a service, the whole service chaining happens automatically. The Orchestrator uses service models, and devices models to auto-generate commands and executes the workflow. If any device is unavailable or fails to provision, the entire service will be rolled back to the previous state to ensure consistency. NSO provides lots of operational support including Packaging & Versioning, Integration into Ecosystem, Upgrades & Maintenance.

Operate

NSO discovers the infrastructure, brownfield service discovery and has vendor plug-ins. NSO introduces self-service through GUI or comprehensive REST API and integrates with ticketing systems. NSO introduces self-service and on-demand provisioning to the network infra and avoids inconsistencies & human errors.

Telemetry / Monitor

NSO constantly streams real-time telemetry data from the infrastructure through audit and reconciliation. NSO validates policy against infrastructure to provide better visibility for SLA assurance. With deep machine learning and correlation, NSO can predict performance and proactively remediate operational issues before they become outages.

What are the minimum requirements for a Network Service Orchestration?

Resource Management Requirements:

- Brownfield Discovery of Services and Devices
- Role Based Access Control at granular user, device and policy levels
- Device Credential Management
- Capacity Management

Service and Device Modelling Requirements:

- Template based service modeling for any device type
- Extensibility to customize device models and service models to match business requirements
- Support various types of device connectivity methods such as CLI, NETCONF, API, etc.

Service Provisioning Requirements:

- Atomic Transactions across multiple network elements with auto-rollback in case of failure in provisioning a single device
- Service Chaining and Service De-Provisioning including shutting down virtual appliances
- Multi-vendor Support
- Zero Touch Deployment

Service Assurance Requirements:

- Config Reconciliation to ensure policy is consistent with underlying infrastructure
- Service Audit and History

Integration Requirements:

- Full REST API for network programmability, provisioning, automation & Orchestration
- Integration with Northbound Systems (OSS/BSS, Ticketing systems, Workflow systems, Self-service portals)
- Integration with 3rd party software (IPAM, DNS, DHCP, Syslog Servers, Netflow collectors, Certificate Managers, VNF Managers, Service Assurance and Analytics software, etc.)

What are the popular applications of Network Service Orchestration?

NSO is independent of the network topology and configuration. However, following scenarios are proven to benefit from NSO.

- Configuring L2 VPN and L3 VPN in multi-tenant environments
- On-boarding 3-Tier applications in a Data Center environment
- Zero Touch Provisioning of Remote Branch office equipment
- Configuring Identity, Access, QOS and segmentation policies in Campus environment
- Interconnecting Service Provider Cloud with 3rd party Public Clouds
- Provisioning Hybrid Cloud for Enterprise Applications
- Security Policy Automation across Multi-Vendor Firewalls
- Load Balancer as a Service

For a detailed description of these applications, check out "How does NSO support various deployments".

How Network Service Orchestration improves Network Security?

While NSO doesn't actively block security threats, it certainly improves the overall security posture of the entire network. For instance, NSO:

- Avoids human errors related to configuration
- Ensures proper roll back of configurations and avoids stray configurations such as ACLs
- Enforces consistent policy across multiple vendor devices
- Captures audit history
- Maintains configuration backup
- Checks compliance and reconciles policy to eliminate config drift
- Enforces Role Based Access Control at granular device, user and policy levels
- Automates multi-vendor firewall policy management.

What role does Network Service Orchestration play in Service Assurance?

NSO provides a single pane of glass for the entire service regardless of the infrastructure differences. For any given tenant, admin can view the service status, provisioned operations, current and historical SLA metrics as well as any alarms related to service health. This information is available through REST API for integration with OSS/BSS for billing purposes.
As part of the YANG service model definition, network architect can define SLA parameters (e.g., which interfaces and metrics to monitor). The YANG model also includes remediation steps when the SLA parameters are not met.

During service provisioning, NSO validates the service model against the existing infrastructure and ensures capacity before provisioning the network elements. The NSO generates commands and APIs for multi-vendor infrastructure as per the recommended best practices. Further, these commands are sent atomically, so if any one device fails to provision, Orchestrator will roll back the configs from rest of the devices.

After service is up and running, admin can schedule periodic reconciliation tasks. NSO uses its service model definition to discover the existing configs and makes sure the policy is consistent with the underlying infrastructure.

NSO constantly collects the SLA metrics, and if any parameters are violated, it executes the remediation steps to automate corrective actions as per the YANG model.

For more on this topic, see
Automate Network Compliance and Service Assurance for Multi-Vendor Network Infrastructure

How to compare multiple NSO solutions?

- Number of Vendors Supported
- Support and Depth of Brownfield
- Discovery and Orchestration
- Support for Physical and Virtual Appliances
- Ease of Customization
- Proprietary or Open Standards
- Scalability
- Validated Service Models
- Ease of using the Development Toolkit

Additional Resource: Listen to the Packet Pushers Podcast for a discussion of evaluation criteria as well as best practices for deploying Network Service Orchestration into existing IT structures.

Comparison with other Networking Concepts and Tools

Config Management Tools - Chef, Puppet and Ansible

Chef, Puppet, and Ansible are ideally suited for Run-book automation for simple and repetitive tasks. Many enterprises have successfully deployed one of these three tools for server automation. They typically bought an enterprise license that covers unlimited nodes. So, at the surface, it makes economic sense to use the same tools for networking.

However, these config management tools are still in their infancy with limited networking vendor support.

For a comprehensive NSO, a YANG model-driven platform approach is needed. For more on this topic, see Network Automation with Chef, Puppet, and Ansible.

SDN and SD-WAN Controllers

SDN controllers introduce programmability, self-service, and agility to a portion of the network infrastructure. Although some network elements are directly managed by an SDN controller, many are not. With a typical network service spanning many layers up and across the network stack including Data Center Access, DC Core, Edge, Campus, Branch/CPE, WAN, etc. SDN controllers typically don't have visibility across the entire stack.

SD-WAN solutions automate the CPE functionality but don’t cover the rest of the network that extends into a large campus/LAN involving routing, security, switching, wireless which requires configuration of QOS, segmentation, port security, and identity-based access policies. Take out the orchestrator, and manual configurations are required for multiple network elements including SDN controllers, OpenStack, VNFs, PNFs, servers, and storage.

A Network Service Orchestrator complements the SDN controllers and helps deliver complete network service delivery across all network domains for your multi-vendor infrastructure.

For more on this topic, see
Super Charge Your SDN Controller with the best NSO

Intent-Based Network Services (IBNS)

IBNS is a new marketing buzzword to describe lifecycle management for network infrastructure. IBNS uses machine learning and advanced orchestration to reduce the complexity of managing network policies.

If Intent Based Networking represents Self-Driving Autonomous cars, NSO represents advanced driver assistance systems such as adaptive cruise control, Collision avoidance, lane change assistance features, etc.

Hence, NSO is the prerequisite to deploying Intent Based Network Services. NSO combined with telemetry data and feedback loops enables Intent Based Network Services.

Network Function Virtualization (NFV)

Service Providers are relying on Network Functions Virtualization (NFV), an ETSI industry specification, to achieve on-demand delivery of network services by avoiding long hardware deployment cycles. ETSI NFV supports dynamic workloads by scaling out virtual network functions (VNF) using industry standard high-volume servers, switches, and storage infrastructure. Further, Network Functions Virtualization (NFV) enables the IT administrator to quickly identify capacity bottlenecks and migrate tenant services for effective resource utilization. However, support for VNF introduces new challenges such as placement, management, and troubleshooting in a multi-vendor environment.

For more on this topic, see NFV Management and Orchestration.

Why select a vendor-supplied orchestration over an open source platform?

Open Source platform allows quick trial and appears economical in the short term. However, the success of any Open Source platform depends on the community support. Current Open Source orchestrators such as ONAP, AT&T's ECOMP, Telefonica OpenMANO NFV have not garnered the critical mass necessary for widespread adoption. Config management tools such as Ansible, Puppet, and Chef have a large community, but they are ideally suited for run-book automation for simple and repetitive tasks. There are also Open Source SDN controllers such as Open Contrail, Open DayLight with limited functionality in the Data Center.

Many organizations start with the Open Source approach, and once they crystallize their requirements, they evaluate vendors against those requirements. The vendors have incentives to adopt latest technologies to offer a scalable and stable platform for their competitive differentiation. However, vendors cater to the majority of users. Hence, if you have a rare mix of network devices or if your service requirements are unique, an out of the box vendor solution will not work.

How does Network Service Orchestration support various deployments?

Use-case 1: Application Delivery Automation

Today's agile organizations rely on IT to introduce new products to market quickly and to differentiate themselves. With the proliferation of Public Cloud, there is enormous pressure on IT to become a service delivery organization.

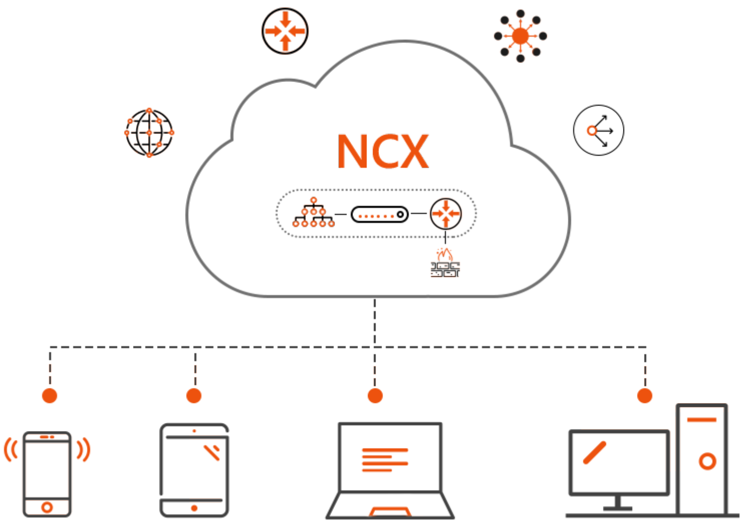
However, legacy systems and manual processes make it extremely challenging to deliver new applications.

Challenges	How NSO Helps
Too many point tools that delay application delivery	Delivers comprehensive network policy automation that supports L2-L7 services including Firewall, ADC, GSLB, WAN Op, Web Proxy, MPLS, QoS, and IPAM
Manual processes resulting in security violations	Includes Role Based Access Control and automated provisioning and de-provisioning as per industry best practices and ensures compliance with regulations
Increasing OPEX to handle change requests from application owners	Introduces Self-Service and enables application owners to make infrastructure changes without IT admin intervention
Managing multiple vendor devices is proving costly	Supports Multi-Vendor devices for each technology in the Data Center and obviates the need to learn multiple vendor GUI or CLI
Many legacy applications preventing adoption of latest technologies	Discovers existing network services and enables self-service automation for them. Relieves the IT admin from trivial network changes and helps them focus on evaluating and deploying new technologies

Use-case 2: Branch and CPE Management

More and more users are bringing personal devices and expect a quality service while many of those services are moving to the cloud.

Hence, IT has the arduous task of enabling application access while ensuring application policy within a shrinking operating budget. The integrated services router and virtual CPE emerged to solve these challenges. However, they introduce new management complexity.

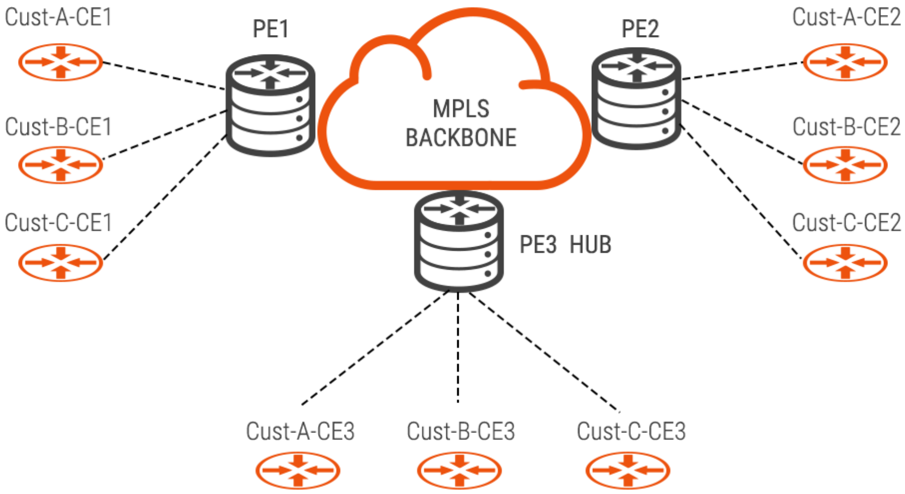


Challenges	How NSO Helps
Need to ensure user experience and security for accessing applications hosted in cloud and data centre	Delivers policy designer that simplifies policy definition for VPN, IPS, Firewall, Proxy, WAN Op, Identity Based Policies, Cloud Web Security
High OPEX due to expensive MPLS backbone connection and frequent policy updates	Introduces self-service and provisions advanced Cisco iWAN features such as DMVPN, Application Visibility, Policy-Based Routing, Performance Routing and minimizes overall OPEX
Need to onboard new branches quickly	Provides Zero Touch Deployment (ZTD) that brings up branches quickly
Need to roll-out new applications and policies quickly at scale	Includes distributed server and agent architecture that enables policy deployment at scale
Troubleshooting branch related issues is very difficult due to lack of documentation, tools and support processes	Provides service to device mapping, real-time health check and threshold-based alerts that simplify troubleshooting effort.

Use-case 3: Provisioning L2VPN

In recent years, the use of Layer 2 Virtual Private Network (L2VPN) transport has helped significantly in simplifying the visible architectures of customer networks while providing the quality of service that customers need.

However, it is expensive to manage a diverse network infrastructure that utilizes complex routing protocols across an ever-increasing footprint.



Challenges	How NSO Helps
Manual per-device CLI Process is slow, error-prone, and requires many hours of vendor-specific learning by engineers.	Automates MPLS L3 VPN, L2 VPN (E-Line, VPLS), EVPN, Wholesales Services using a vendor agnostic service model using a self-service GUI.
Managing hundreds of devices from Multiple Vendors is expensive and inconsistent.	Orchestrates CE, PE, P and RR nodes from Cisco, Ericsson, Juniper, Fortinet, Alcatel, Huawei, etc. as per unified service model that is consistent across vendors and platforms.
Tracking, Documentation, and Troubleshooting complex network policies is a nightmare.	Streamlines Day-1-N MACDs for IGP domains, ACLs and QoS Policies.
Expensive to meet auditing and compliance requirements.	Automatically captures audit logs and periodically runs compliance checks to ensure device configuration matches network policy.

Use-case 4: Interconnecting multiple Clouds

Cloud Gateway enables managed enterprise customers with private and dedicated connectivity to multiple cloud platforms. The solution offers end-to-end service including data carriage, configuration, and support. Cloud Gateway presents a simplified self-service portal for customers to decide their choice of cloud and within minutes the infrastructure is provisioned with improved security and application performance.

Challenges	How NSO Helps
Manual process to configure complex routing protocols is cumbersome, expensive and error-prone	Orchestrates L3 Interfaces, VRFs, Q-in-Q tagging, BGP, Static Routes, QOS, Day 1 Configuration, Smart Licensing, Prefix lists, Access Lists, Route Policies and Selective Route Leaking
Frequent change requests (MACDs) resulted in human errors	Delivers a self-service portal so that customers can order new services, monitor and modify existing services as well as terminate services on-demand
Rapid innovation requires a flexible platform approach to keep up with new architectures. Each Cloud Provider (Azure, AWS, vCloud Air, etc.) has its own methods and limitations of supporting the internet peering.	Models various connectivity scenarios without requiring constant software patches. The operations team is expected to update the service definition on-the-fly without vendor help

Use-case 5: Multi-Vendor Firewall management

The Internet is full of horror stories related to denial of service attacks and data breaches caused by configuration errors in firewalls. A consistent approach to multi-vendor firewall management improves overall security posture and reduces OpEx.

paloalto NETWORKS
vmware
cisco
Check Point
JUNIPER NETWORKS
FORTINET

Challenges	How NSO Helps
Network and Security teams work in silos resulting in a disjointed process to deliver end-to-end network services	Provides service-level view including Firewall, Load Balancers, Routing, Switching, LAN/WANs. End-to-End service chaining ensures applicationReachability.
Firewall rule management is inefficient and error-prone due to homegrown legacy tools	Provides discovery, configuration management and monitoring capabilities for different vendor firewalls. Simplified firewall rule management reduces operational overhead.
High volume of change requests result in gigantic firewall rules, application-identity mappings, router ACLs	Manages thousands of firewalls rules on hundreds of devices for different use cases such as perimeter security for public clouds and enterprise private clouds, ACL management in huge carrier networks, etc.
Managing multiple vendor devices is proving costly	Efficiently orchestrates firewalls from Cisco, Checkpoint, Juniper, Fortinet, Palo Alto Networks, VMware from a unified web interface.

Use-case 6: Managed Service Provider Solutions

Cloud-based application delivery has transformed enterprises of all sizes. Network access is critical to the viability of today's businesses. As the trend to outsource network management continues, Managed Service Providers have a lot of market opportunities ahead. But, they need to ensure scalability and stability of their offerings while reducing OPEX (Operational Expenses).

Challenges	How NSO Helps
Need to support network policy deployment for branch, campus and data center for enterprises of all sizes	Supports network policy deployment for enterprise branch, campus and data center of all sizes using the distributed server and agent architecture.
Need to provide value-added services and demonstrate ROI to customers	Delivers value-added services such as self-service, pay-as-you-grow scalability, branch on-demand, etc.
Need to build expertise to onboard new customers quickly	Offers intuitive policy designer that enables quick-service definition and faster onboarding of new customers.
Manual process for change requests and support costs increase OPEX	Includes Service Manager that simplifies troubleshooting efforts and introduces self-service that avoids MSP involvement for change requests
Different customers have different choice of vendor devices across each technology	Supports industry leading vendors – Brocade, Cisco, Citrix, F5, Fortinet, BlueCoat, Checkpoint, Palo Alto Networks, VMware, etc

anuta networks

http://www.anutanetworks.com/

info@anutanetworks.com