Simplify Virtual Network Function (VNF) deployments for WAN sites with Nuage Networks SD-WAN

Traditional enterprise Virtual Private Networks (VPNs) are expensive, difficult to modify and adapt to new requirements, as well as time-consuming to establish. VPN equipment or customer premises equipment (CPE) has also traditionally been proprietary with integrated control and management services on each device. This has introduced complexity and increased administrative overhead. VPN services can also be dependent on service location and accessibility to carrier networks, increasing complexity for global deployments. Delays from weeks to several months to deploy corporate VPNs are all too common.

The advent of SD-WAN revolutionizes VPN service offerings

Software defined wide area networking (SD-WAN) evolved from data center and cloud technology to alleviate many of these bottlenecks to VPN services and to drive automation of VPN service delivery.

In the SD-WAN model, software-based policies are centralized in the cloud rather than managed box by box. This approach helps to automate IT processes and accelerates time to optimize and update network services. The proprietary, high-overhead CPE is replaced with a cost-effective, open x86-based appliance, including white box switches. SD-WAN also provides consistency across a range of network transport technologies, including traditional MPLS networks, internet broadband, and 4G LTE cellular services at any location. The end result is a lower cost VPN service, dynamically managed and optimized through centralized policies, running on commodity hardware and commodity networking services.

Challenges with adding network services

Enterprise networks have a need for a range of layered security and application services, such as firewalls, intrusion prevention systems (IPS's), Quality of Service (QoS) managers, as well as wireless LAN (WLAN) controllers. The traditional model for delivering these services to remote WAN sites is through additional appliances deployed at the branch site or hosted in the data center. They, too, are managed node by node, complicating VPN deployments and application access and delivery. Even cloud-provided complementary services are integrated through manual stitching, a tedious process that requires defining pre-determined routing paths to the appropriate service device or location. The lack of flexibility leads to vendor lock-in and high operational costs.

SD-WAN enables a new services integration model

Enterprises want value-added services in the cloud consumption model. This means automated, on-demand, programmable, and managed and provisioned services through a centralized policy repository/controller.

Enterprises also need a holistic approach to deliver value-added services by providing them in flexible locations, either locally or cloud-hosted. Policy management of these services should be integrated with the software defined network management and control plane, rather than as standalone management consoles. When there are multiple deployment models for services (local or cloud-hosted), there needs to be a uniform policy across different modes for consistency and ease of administration. Latest generation SD-WAN offerings, such as those from Nuage Networks, are allowing telco operators to deploy advanced services and application networks to delivery much greater QoS — on-demand, at lower cost.

Service chaining, the ability to sequence multiple network services, such as the firewall and load balancer in an application network or VPN, comes in two modes:

- Integrating centralized cloud-hosted services hosted in the CO/PoP or data center, or to cloud hosted SaaS security services, which are chained to a cloud-hosted service, such as Zscaler.
- Hosting VNF services on the CPE appliance at the remote WAN location as part of a multi-purpose or universal CPE.

To illustrate the flexibility and consistency of the Nuage Networks SD-WAN platform, a comparison can be made between how VNFs can be chained into WAN networks by enterprises or through service providers and how VNFs can be hosted in the cloud, or locally on the CPE appliance.

Use case 1: Centralized services

To implement a uniform network and services policy from the WAN to the data center, a multi-tenant and highly scalable overlay fabric is required. The challenge with remote service chaining to centralized services is that the WAN and data center are two separate domains, often running over separate networks, providers, and protocols. There is no easy way to stitch together networks based on VXLAN over IPSec or other IPSecs on SD-WAN, and VXLAN in the data center. Rules must be manually defined at the Provider Edge (PE), or data center gateway to connect the two domains. From a control plane perspective, they are separate domains and policies .

The Nuage Networks SD-WAN platform solves this problem with an integrated policy and seamless control on a single platform. From the branch location, the service chains refer to a VM endpoint in the data center and redirect to it. This enables a policy that spans the entire domain — from the WAN to the back-end application. The unique network automation platform for both data center/cloud and WAN allow Nuage Networks to provide an integrated service chaining capability, as show in Figure 1.

Use case 2: Universal CPE

VNF services can also be deployed and chained directly on the WAN CPE appliance, generally referred to as a "universal" CPE. The initial available services are part of the base SD-WAN routing and forwarding software available from Nuage Networks. Examples include Network Address Translation (NAT), Dynamic Host Control Protocol (DHCP), Layer 4 Access Control Lists (ACLs), Layer 7 ACLs, URL filtering, and IPS. In the case of a small branch device, where there are no resources to host more value-added functions, the initial embedded services may offer a minimum tier of default services from providers. This approach can be complemented by service chaining to remote services in the cloud.

An additional option is providing hosted on-premises services on the branch CPE. Our approach is to provide all the functionality required for networking in a branch environment in a single form factor along with a unified policy (a "branch-in-a-box" model). The virtualized services can be VMs or containers. While the services market for firewalls, session border controllers (SBCs), and WAN optimization is based on VM software, applications such as file servers and print servers could be run as containers. Customers should be able to select the right footprint and software form factor for the CPE-hosted services.

FIGURE 1. Nuage Networks SD-WAN: A unified and flexible platform for branch VAS

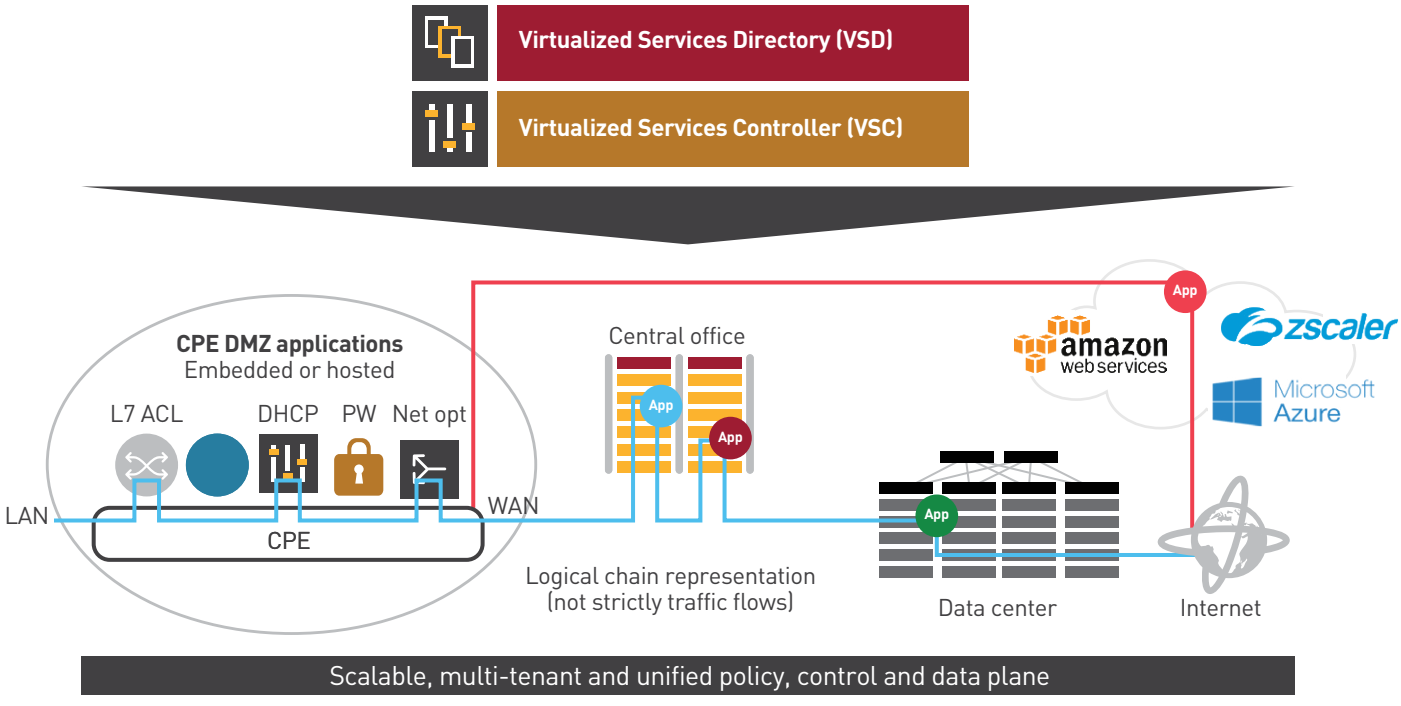
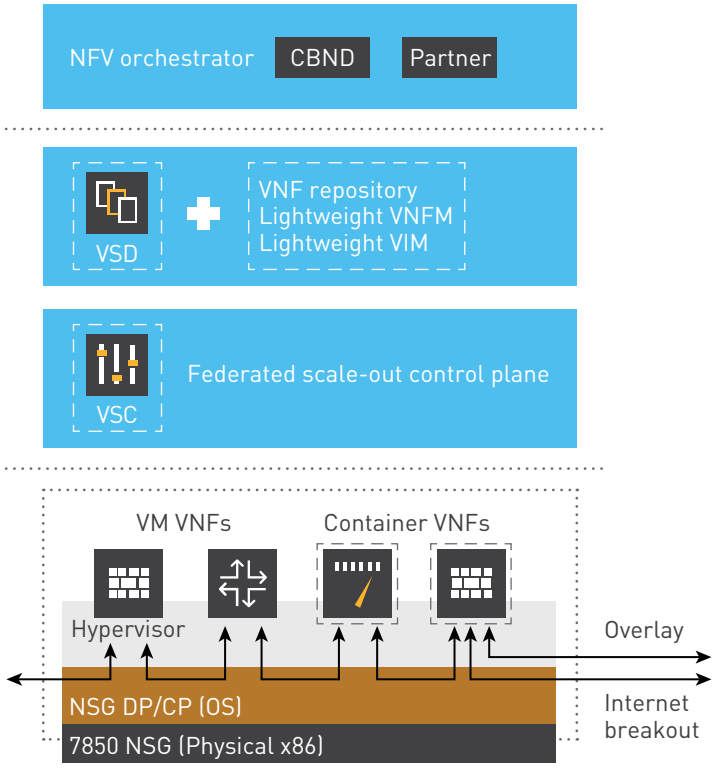


FIGURE 2. Solution architecture for hosted VNFs



- REST API-based integration with NFV orchestrator

- VNF onboarding, catalog management
- Lightweight VNF lifecycle management
  - Light weight VIM (scheduler)
  - VM instantiation/deletion/default configure
- Service chaining framework
  - VNF insertion in packet flow
  - Advanced forwarding rules to redirect traffic

- KVM hypervisor/Libvirt management of VNF
- Resource monitoring and VNF health checks

The Nuage Networks SD-WAN platform can be viewed as a stack of networking orchestration, management, and delivery services. The Virtualized Services Directory (VSD) and the Virtualized Services Controller (VSC) make up the Virtualized Services Platform (VSP), or the SDN/SD-WAN centralized controller software. The lower box shows the CPE appliance at the WAN site, with embedded services and platform software on the x86 device.

At the bottom of the CPE stack is a hypervisor or, in the case of container, a Docker engine is run that is used to host a range of VNF services. Resource monitoring and VNF health checks are localized to the CPE. The communication channel is secure and is the same one used by the SD-WAN controller, which is also secure, tamper proof and used for booting and pushing forwarding rules.

Above the CPE in the VSP controller is the policy plane. The policy plane for SD-WAN is extended for the VNF catalog of services and lightweight lifecycle management, such as creation, deletion, and upgrading. VNF policies are self-contained in the Nuage Networks VSP software stack.

Policy comes in two parts:

1. Where and when a VNF needs to be deployed.
2. What kind of application traffic goes to which VNF, as well as how to do local traffic chaining.

Visibility of application traffic types and of services required to support each application is an important part of the SD-WAN VNF model. It is also an important aspect of the policy definition language, which needs to align with application requirements.

Integration to higher level orchestration and operations support systems/business support systems (OSS/BSS) is implemented above the control and policy plane layer. This is where business services are defined. Integration into the policy plane is provided through open REST APIs. The deployed architecture is also highly scalable because centralized orchestration policies can be pushed out as needed through the controller rather than on a node-by-node basis for each CPE endpoint.

Architecture highlights

Secure deployment of VNF

The communication channel used for VNF management is an extension of the SD-WAN controller. It is secure, tamper proof, and is used for booting and pushing forwarding rules. The channel is also a secure, isolated, well-contained infrastructure for hosting VNF services.

Scalable solution

The VNF management actions are defined centrally and enforced locally at the CPE. The distributed processing allows the architecture to scale to large deployments. For local service chaining, the SD-WAN platform provides the forwarding to and from the VNF. There is no separate forwarding VNF and there is no tromboning involved.

Policy plane

The policy plane for SD-WAN is extended to handle the VNF catalog and a lightweight VIM lifecycle to integrate services policies with network policies, which simplifies deployments.

An Open VNF platform

The solution can support any hosted VNF — from multiple vendors across a range of service categories. Other SD-WAN vendors provide only their VNFs, not those from third parties. As a result, there is no vendor lock-in or lack of flexibility.

Integration with higher level orchestration

The architecture provides a well-contained solution that provisions an end-to-end network service rather than just a VNF hosting platform. This can be integrated to external orchestration platforms using REST API. The centralized orchestration platform does not have to update and provision on a node-by-node basis for each of the CPE endpoints.

Summary

The Nuage Networks approach to virtual application services provides service level orchestration of VNFs hosted in the branch and seamless service chaining for services hosted in the data center/PoP. The result is a holistic solution for next generation branch infrastructure. Benefits include:

- **Increased agility:** Functionality of multiple appliances provided in a single network element accelerates time to deployment. Customers can roll out branch-in-a-box in a matter of minutes and eliminate the provisioning time and hardware dependency of appliances.
- **Reduced complexity and TCO:** Customers can significantly lower OpEx by reducing or eliminating branch-office truck rolls, using standardized hardware and easily integrating new services into existing appliances. New services can be rolled out with a single click along with seamless insertion and chaining of virtualized services on the premises and in the cloud.
- **Best-of-breed security and other hosted services:** Customers can continue to leverage the investments made in their security vendors and need not retrain employees on new solutions. The security platforms can be migrated from appliances to virtualized form factors integrated into their SD-WAN enabled branch.