Meeting the expectations of digital shoppers with SD-WAN

Design principles for transforming retail networks

White paper

nuagenetworks
From Nokia

Contents

Introduction

Today the demand for digital business transformation is especially present in the retail sector. With over 90 percent of pre-purchasing research happening online and an on-going decline in brick-and-mortar sales, retailers are continuously looking for ways to respond to new shopper expectations. They are especially concerned to bring the same conveniences available online to the in-store shopping experience.

For shoppers, in-store Wi-Fi and personal smartphones and tablets are providing them with a mobile e-commerce connection that can be blended with their in-store experience. Branch stores can use various technologies, including RFID, smart signage, beacons, mobile POSs and video analytics, to further enhance the in-store shopping experience. These and similar technologies also have the potential to reduce the costs of managing this enhanced retail experience.

All of these digital technologies rely heavily on the network and the cloud to perform their magic. Most retail networks are not configured to handle either the bandwidth needs or the security and reliability requirements of these new mission-critical, real-time applications. Most retail chain IT departments are also not equipped to rise to this new level of performance using traditional networking tools.

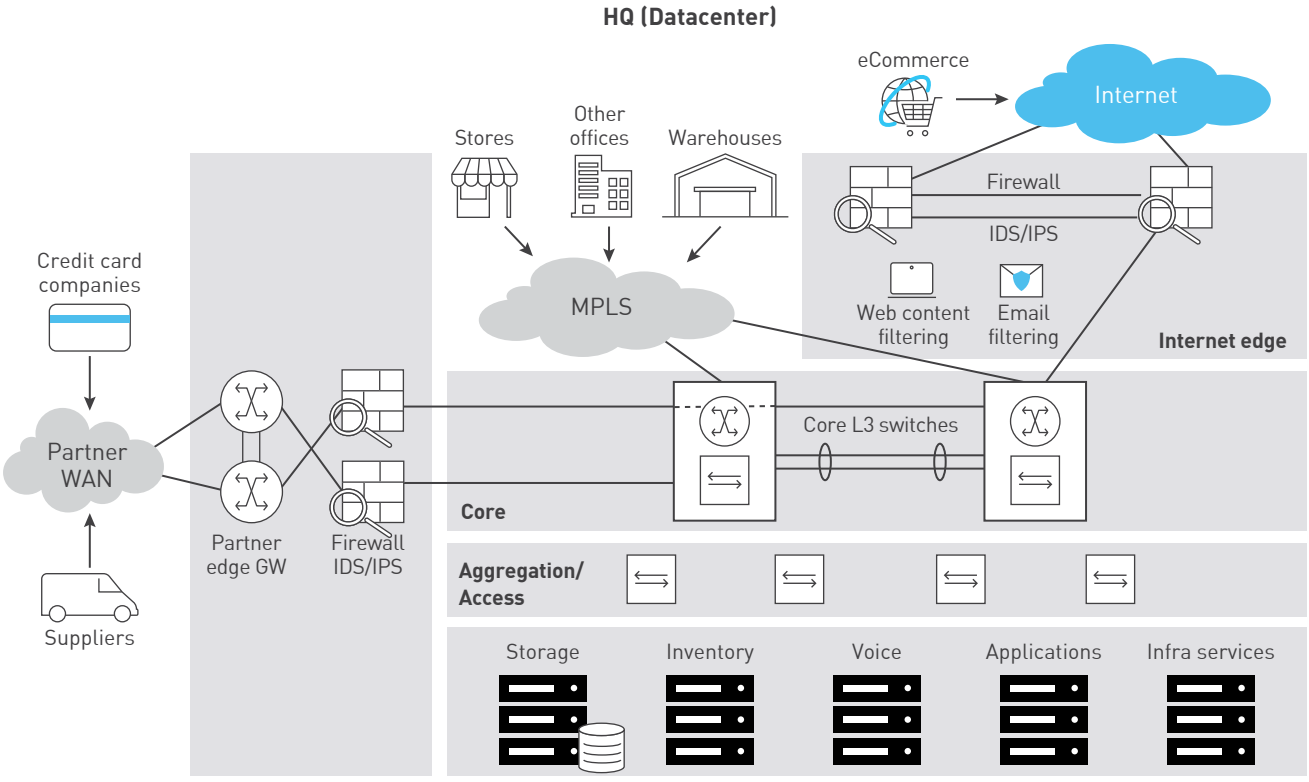
Fortunately, software-defined networking (SDN) and virtualization solutions, which made their impact first in the datacenter, are now available for distributed enterprise networking across the wide area network (WAN). Dubbed SD-WAN, these solutions make it possible for retail chain IT departments to manage networks of hundreds and even thousands of branch stores using software tools that simplify setup and automatically provision, configure and manage of WAN connections to seamlessly connect branch stores, on-premises datacenters, and private and public clouds.

In this document, we will describe a typical retail chain IT architecture and explore the main technical challenges that the retail industry is facing in digital business transformation. We will look at the Nuage Networks SD-WAN 2.0 solution as a possible way to meet these new challenges. Finally, we will discuss various ways to design and architect a retail chain network that can cost-effectively and efficiently support the new connected-shopper experience.

The retail chain network design

A typical retail chain's IT system consists of multiple parts, some of which are geographically dispersed. The essential part is the main datacenter, which contains all the business and infrastructure applications required for day-to-day operation. It is also the destination for many connections originating from remote locations such as retail stores, branch offices, warehouses, partner systems and e-commerce applications. Depending on the performance and security requirements, the WAN transport for these remote locations is either private MPLS circuits or broadband internet connections. A sample retail chain network is depicted in figure 1.

FIGURE 1. A sample retail chain network



The retail chain headquarters is where centralized data processing takes place and where various subsystems responsible for administrative and service functions exist. These functions can be grouped into different layers that are outlined below.

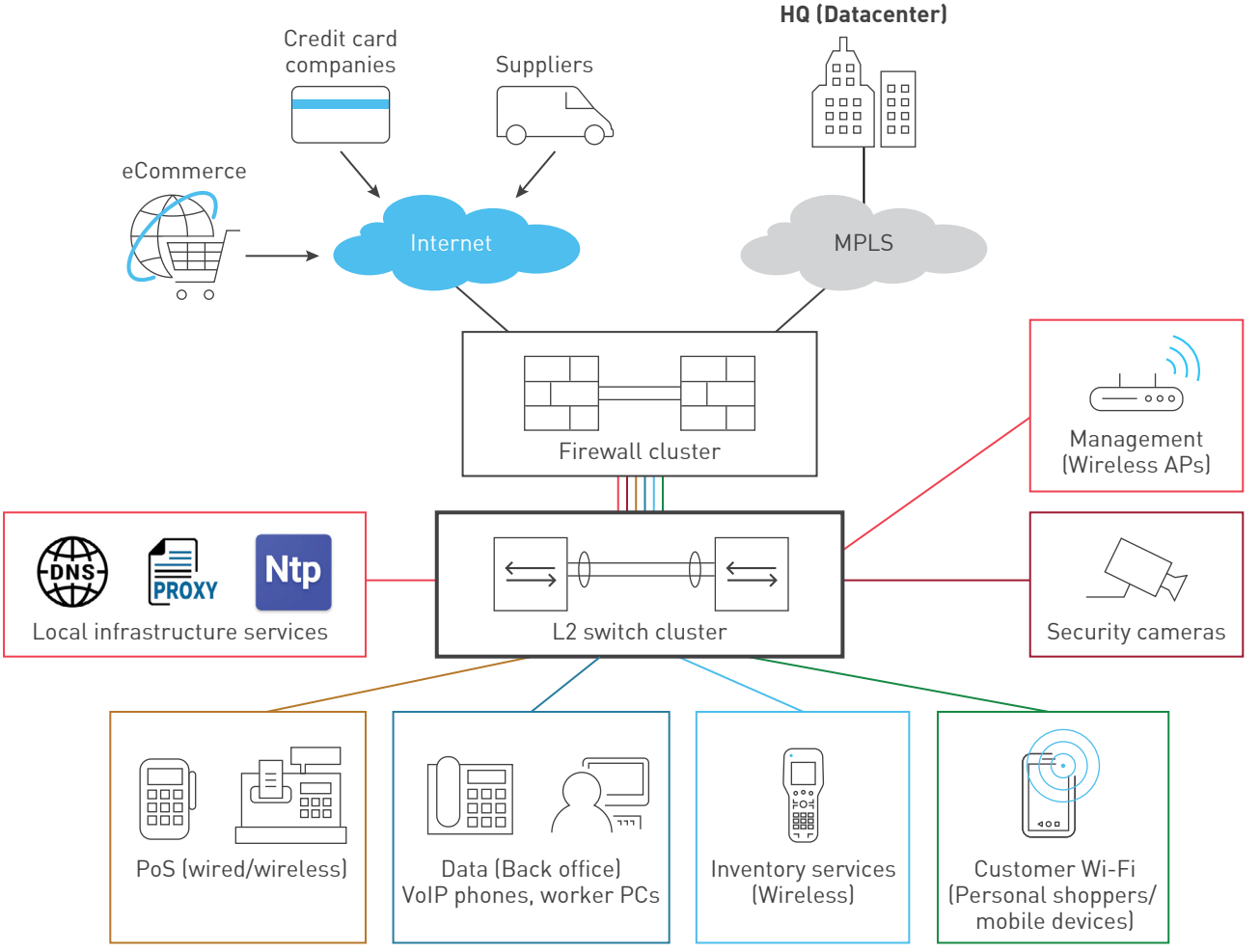
- **Core layer –** As its name suggests, the core layer provides a high-speed packet switching backplane for all data-center systems. It doesn't implement any firewall functions; its only purpose is to transport data from one subsystem to another as fast as possible. This is usually implemented using high-speed layer three (L3) switches.
- **Aggregation/access layer –** Depending on the size of the retail-chain (small/medium/large), the access/aggregation layer can either be implemented as separate aggregation and access layers, or implemented using the same equipment in a single layer. In either configuration, it represents a repeatable template for scaling applications and services within the datacenter. It is typically implemented in the form of a top-of-rack (ToR) L3 switch block and can be multiplied as many times as needed for scaling.
- **Infrastructure/servers layer –** This layer contains all the physical endpoints: storage, virtualization, voice and application servers. They are all connected to the ToR switches and host the infrastructure and business applications.

- **Internet-edge layer –** This is the zone providing internet connectivity to the whole group. It hosts infrastructure services, email and web content filtering and also an advanced firewall/IDS/IPS layer for deep-packet inspection (DPI). This ensures that the incoming internet connections are secure. This zone can also provide internet access for applications from the remote branches and offices.
- **Partner-edge layer –** Similar to the internet edge zone, the partner edge is a DMZ providing connectivity to different partners such as the different credit card companies and suppliers. A firewall/IDS/IPS layer is also present to inspect incoming traffic from the different partner systems or networks.
- **MPLS WAN –** The private MPLS network is a trusted zone used for connectivity with other entities belonging to the retail chain such as retail stores, remote offices and warehouses.

Branch store network

The typical network design of a branch store will depend on the size of the branch (small/medium/large) and may contain several or all of the subsystems depicted in figure 2.

FIGURE 2. Typical branch store network.



L2 switch cluster – Typically, the L2 switch cluster includes a pair of switches that connect all network devices at the branch. They provide L2 connectivity and VLAN segmentation for the different subsystems.

Firewall cluster – This cluster includes firewall appliances used to provide security between different subsystems as well as filtering internet access. They also route traffic between the different subsystems.

Local infrastructure services – Local infrastructure services include DNS, proxy and NTP that are used by all local devices.

Wireless management subsystem – A dedicated VLAN, for the management of the wireless access points, is installed in the store or remote office.

Security cameras subsystem – A dedicated VLAN exists for the management of the video surveillance equipment installed in the store.

PoS (wired/wireless) – VLANs are dedicated for wired and wireless point-of-sales (PoS) devices.

Data (back office) – Dedicated VLANs host back office equipment (e.g., PCs, printers, VoIP phones).

Wireless inventory services – Dedicated VLANs exist for wireless inventory equipment.

Guest Wi-Fi – These are dedicated zones for guest Wi-Fi access such as shoppers using smartphones or tablets.

Since some stores provide customer Wi-Fi access, it almost goes without saying that security measures must be put in place to ensure complete protection and isolation of corporate subsystems and data. This function is provided by the switches (L2 VLAN segmentation) and firewalls (L3-L4) using security policies.

Typical traffic flows in branch store

In order to function properly, a branch store requires secure connectivity to systems and applications in other parts of the retail chain network. Below is a list of typical traffic flows used by branch store applications and services:

- Connectivity to credit card payment networks (e.g., VISA, MasterCard, AMEX) for PoS terminals (typically over internet)
- Connectivity to supplier networks and systems by back-office PCs (through internet directly or via the MPLS network through HQ)
- Guest Wi-Fi user access to eCommerce resources such as retailer websites (typically over internet)
- Business application traffic to the HQ central office and datacenters using the corporate MPLS network.

Challenges with current retail chain IT systems

We have seen that a retail chain network can have an extremely complex IT system. While being critical to business needs, this complexity makes it difficult to manage. Below are some of the most common technical challenges facing IT admins of these systems.

Lack of centralized network management

We have described a large number of network-connected devices, even in a single branch store. Multiplying this by several hundred stores, in the case of medium or large retail chains, makes for a potentially overwhelming number of devices that network engineers have to manage. One of the main challenges is ensuring configuration consistency across all network devices in the different store locations.

WAN link resiliency and load-balancing

Retail stores need highly available and reliable network connectivity in order to be able to process sales transactions. Network downtime due to WAN link failure is unacceptable and needs to be minimized. Multiple WAN circuits can be provisioned, but one needs to make sure that a proper automated fail-over mechanism is employed. It may also make sense to distribute the traffic across the multiple WAN links to avoid under-utilization of circuits.

Compliance with payment-card-industry data-security standards (PCI DSS)

Today nearly 90 percent of the payments in the retail industry are done using payment cards. Yet the threat of a breach or compromise continues to be a real concern for all banks and merchants. The PCI Security Standards Council was established in 2006 to define a standard framework that would safeguard credit card data and reduce fraudulent transactions. Retailers must ensure that the network solution achieves PCI DSS compliance.

Security isolation of different zones inside the branch

Different zones inside the branch and across the retail chain network have different security requirements. PoS terminals, infrastructure services and back office applications are highly sensitive and need to be isolated from the less sensitive ones such as guest Wi-Fi, for example. Independent, application-aware security policies need to be defined and maintained inside each branch and across the entire network. This process is labor-intensive, complex and error-prone.

Ensure optimal application performance

Different applications have different performance requirements. Some need to be prioritized over others and doing this manually is cumbersome and inefficient. A networking solution that is capable of recognizing application signatures and SLA requirements, and assign application flows to different traffic classes based on their performance needs, greatly simplifies this process and helps optimize and guarantee performance.

Lack of network visibility

Today's traditional WAN doesn't provide efficient statistics. The lack of statistics doesn't allow planning for improved user experience. Having this information is vital to properly understanding and managing network, performance and security issues.

Extremely long WAN-circuit provisioning times

When a new store location is created, it may take weeks or even months to provision internet/MPLS circuits. During this time the store cannot operate, which has significant business impact.

These are some of the most common challenges that the retail industry is confronted with during the digital transformation phase. In the following sections we will address these challenges using an innovative solution from Nokia's Nuage Networks™.

Nuage Networks SD-WAN Solution

Solution overview

Nuage Networks Virtualized Network Services (VNS) is an industry-leading SD-WAN 2.0 solution. VNS automates the provisioning, configuration and management of WAN connections to ensure optimal quality of service (QoS) at the lowest cost, all the while meeting strict business policy and security requirements for each application. VNS provides this policy-based automation across the WAN, using broadband internet and/or provider-managed VPNs, to seamlessly connect branch stores, on-premises datacenters, private and public clouds.

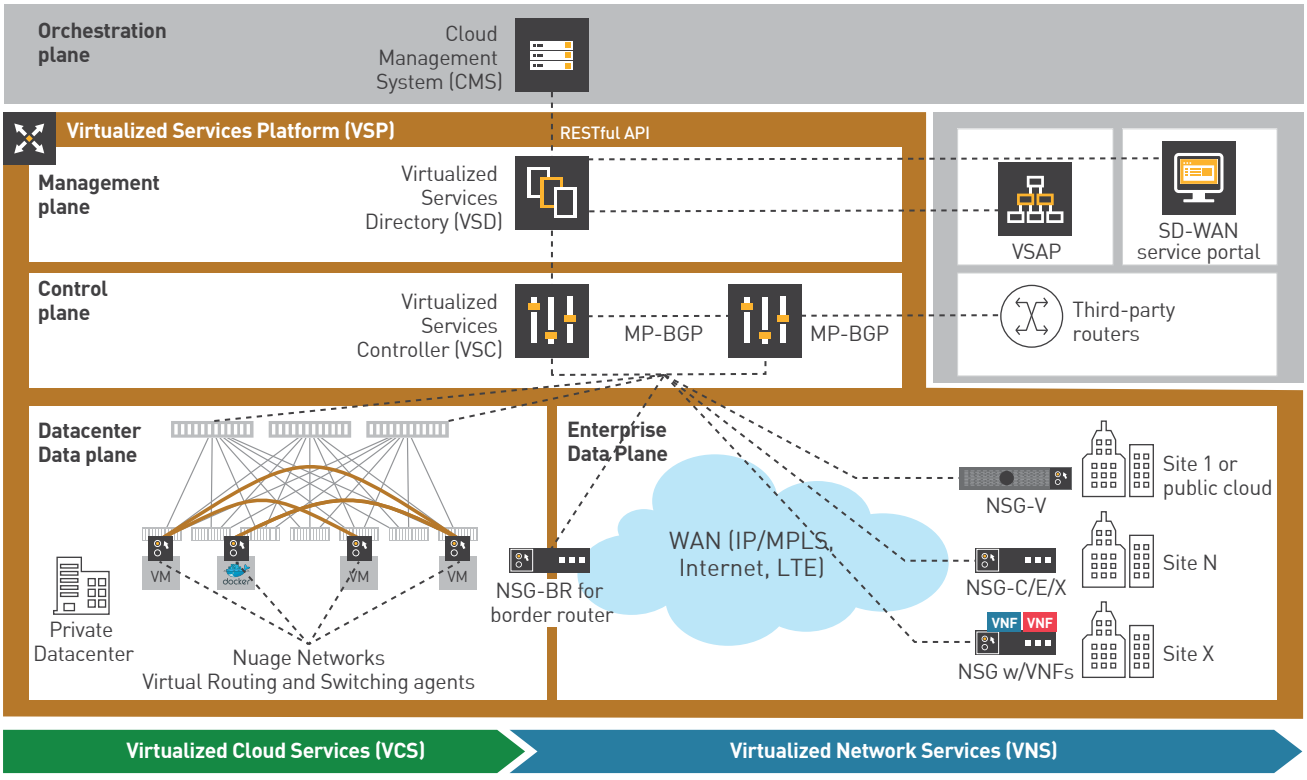
VNS relies on a central policy repository to define business- and application-specific rules that dynamically optimize WAN links and remote branch appliances or devices. With VNS, the SD-WAN-enabled network is dynamically optimized to route traffic governed by specific application policies or by the most cost-effective

network path to meet each application's performance criteria. For example, VNS can immediately drive down expensive WAN costs by leveraging commodity internet broadband, LTE or other low-cost WAN uplinks whenever possible for certain applications. As another example, VNS can leverage LTE transport as a back-up transport link for application resiliency programmed on a per-application basis.

Because VNS has no requirement for expensive proprietary branch hardware, both remote hardware and management costs are reduced. VNS can also simplify branch store networking by consolidating multiple network functions, such as load balancing, service chaining, security services and other network functions into a single virtualized platform. With automation capabilities from VNS, the tedious, time-intensive tasks associated with setting up a new branch store and/or VPN service connectivity can be reduced from several weeks to only a few minutes. Retail chains have greater flexibility to customize their VPN service on-demand, while eliminating IT overhead at remote sites.

The Nuage Networks VSP solution architecture has four key elements (figure 3).

FIGURE 3. Nuage Networks VSP architecture



Virtualized Services Directory (VSD)

A programmable policy and analytics engine. It provides a flexible and hierarchical network policy framework that enables IT administrators to define and enforce resource policies in a user-friendly manner. VSD contains a multi-tenanted service directory that supports role-based administration of users, compute and network resources. It also manages network resource assignments such as IP and MAC addresses.

For service assurance, VSD allows the definition of sophisticated statistics rules such as collection frequencies, rolling averages and samples, as well as threshold-crossing alerts (TCAs). When a TCA occurs, it will trigger an event that can be exported to external systems through a generic messaging bus. Statistics are aggregated over hours, days and months and stored to facilitate data mining and performance reporting. VSD can be deployed as a stand-alone or clustered solution depending on scaling needs.

Virtualized Services Controller (VSC)

The industry's most powerful and scalable SDN controller. It functions as the robust network control plane for datacenters, maintaining a full view of per-tenant network and service topologies. Through VSC, virtual routing and switching constructs are established to program the network forwarding plane using the OpenFlow™ protocol. Multiple VSC instances can be federated within and across datacenters by leveraging MP-BGP — a proven and highly scalable network technology.

Virtual Routing and Switching (VRS)

An enhanced Open vSwitch (OVS) implementation that constitutes the network forwarding plane. It encapsulates and de-encapsulates user traffic, enforcing L2 to L4 traffic policies as defined by VSD. VRS tracks virtual machine (VM) creation, migration and deletion events to dynamically adjust network connectivity. VRS supports multiple hypervisors and container-ready platforms in virtualized server environments. It also operates as a gateway for bare metal servers or service appliances.

VCS also includes a physical network appliance, the Nuage Networks 7850 Virtual Services Gateway (VSG), that serves as an overlay network tunnel endpoint where needed, for example, when integrating with physical servers. It also works with leading networking vendors' top-of-rack switches for VXLAN termination. To support bare metal applications, a software VRS-B (bare metal) may also be deployed directly on the physical server, avoiding the need for a VXLAN-compliant top-of-rack switch.

Network Services Gateway (NSG)

The NSG provides service demarcation and network functionality at the branch, based on x86 COTS hardware. Depending on the throughput needed, it can be physical (NSG-P: Physical Network Services Gateway, Nuage Networks provided x86 hardware) or virtual (NSG-V: Virtualized Network Services Gateway, customer provided x86 server).

How the Nuage Networks SD-WAN 2.0 platform can help

In the previous sections we described in detail the typical retail chain's network and highlighted the most common technical challenges. We will now focus on explaining how the Nuage Networks SD-WAN solution can help address most of those challenges by providing a universal, flexible and scalable network solution.

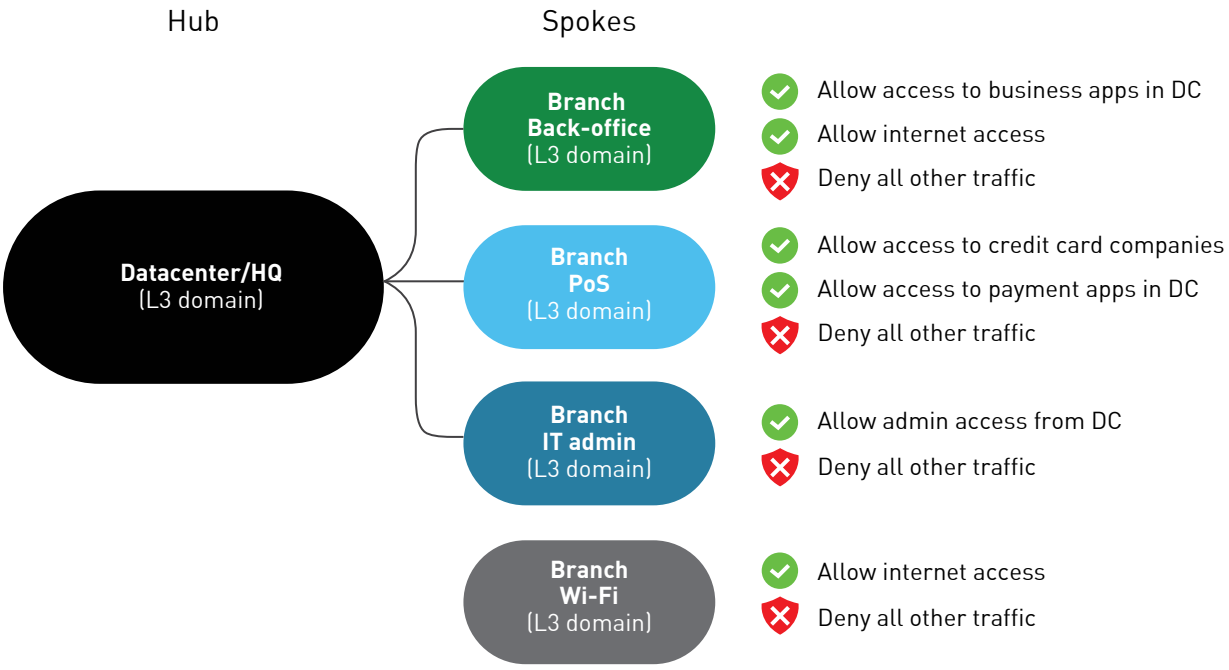
Comprehensive centralized network management

Being a software-defined networking (SDN) solution, the VSP provides a centralized management layer, implemented by the VSD. The main features of the VSD are:

- Full multi-tenancy, with support for overlapping IP addresses and per-tenant role-based administration
- Northbound APIs, with support for integrating the leading cloud management platforms (e.g., OpenStack, VMware, Hyper-V, Kubernetes, Mesos)
- Built around the concept of "define once and reuse multiple times".

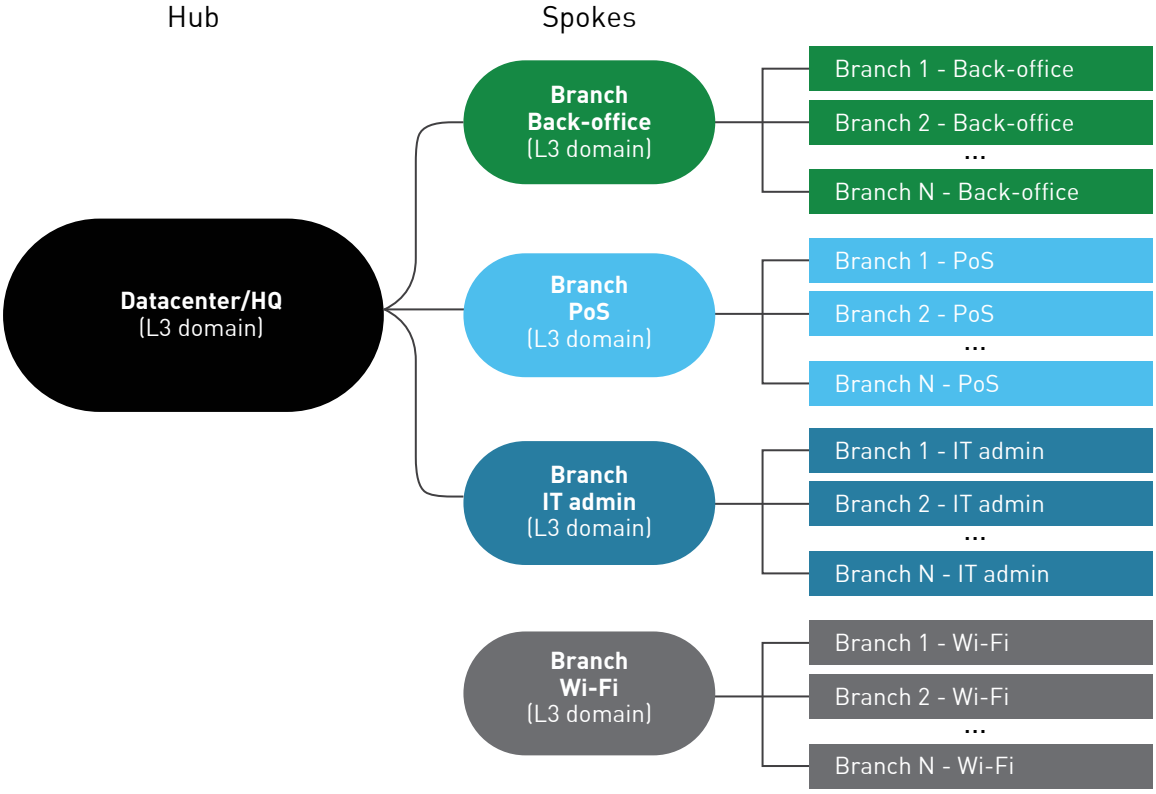
The Nuage Networks VSD can be used to create network templates using simple constructs such as subnet, zone and L3-domain. One possible method of building the virtual branch store infrastructure is to define several isolated domains for different branch subsystems such as back-office, points-of-sale, IT admin, user-Wi-Fi, as well as their associated security policies.

FIGURE 4. Defining sub-systems and security policies for the branch store.



Once the logical constructs have been created and the security policy defined, they are linked to the datacenter in a hub-and-spoke topology and are ready to host branch zones and/or subnets.

FIGURE 5. Hub-spoke topology for sample branch store.



The provisioning of a new branch consists in adding the necessary zones/subnets to the corresponding L3 domains and connecting the NSGs to them. Once the subnets and zones are added, they will inherit the defined security policy from the L3 domains.

Another important aspect related to centralized management is the easy bootstrap process for CPE. Bootstrapping enables CPEs to connect to the control plane components (VSCs), download their service configuration, and connect end-users to their services based on pre-defined policies with minimal user interaction.

When a new branch is opened, the CPE device is shipped to the remote location. Once received, the CPE can be activated and setup using any of the following bootstrapping options:

- **Zero-factor bootstrapping:** The person tasked with installing the CPE plugs a USB flash drive provided by the network administrator into the CPE to start the bootstrapping process
- **One-factor bootstrapping:** The person that installs the CPE receives an email with an activation link, which if clicked on while connected to the CPE, initiates the bootstrapping process
- **Two-factor bootstrapping:** The person installing the CPE similarly receives an e-mail with an activation link, and additionally, an SMS message is sent to their mobile device as a second-factor authentication.

This feature automates the activation process and avoids having a qualified engineer travel to the retail store to activate the NSG. It is possible for any branch employee to complete the bootstrapping tasks.

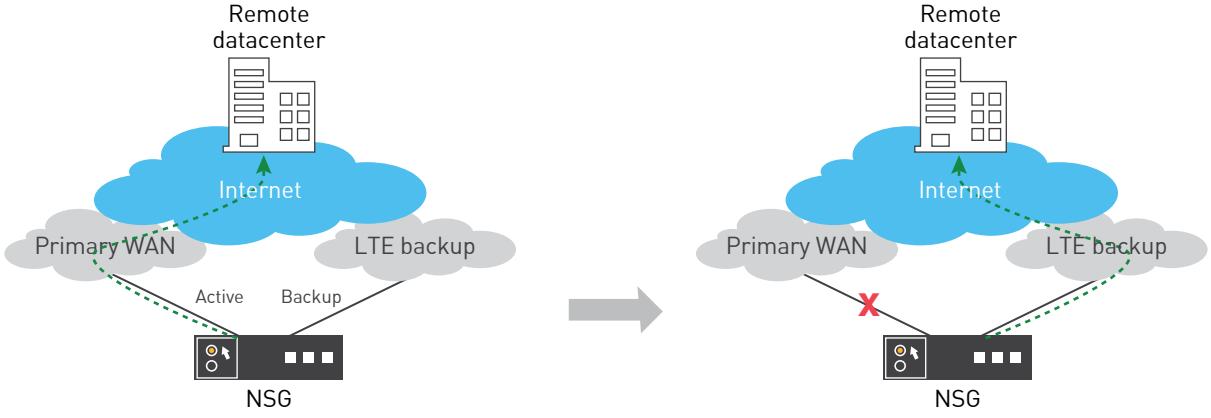
WAN link resiliency and load-balancing

To ensure an "always-on" WAN connection, it is possible to provision multiple WAN access points. There are two important aspects to consider when designing such a solution:

1. The CPE device needs to support multiple WAN uplinks and ensure a proper failover mechanism to work around faults and service disruption.

   The Nuage Networks NSG CPE supports multiple WAN uplinks and WAN access types that include broadband internet access, MPLS and LTE. In the event of a link failure, the CPE device will automatically switch over all flows to a different link. When the failed link is restored, the NSG will automatically restore the switched flows and connections to the original link.

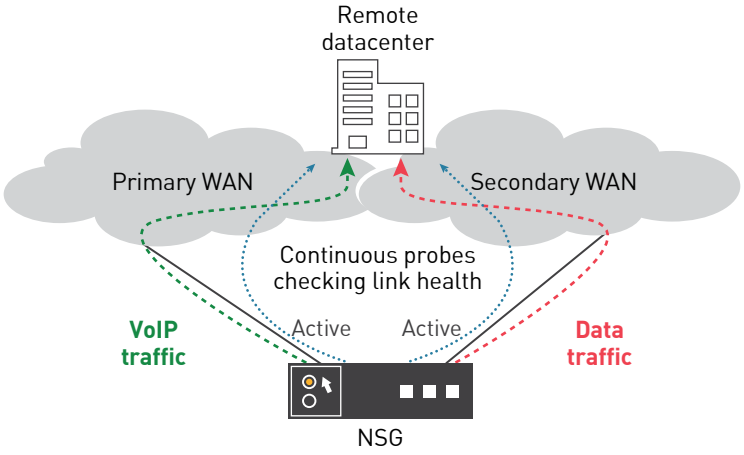
FIGURE 6. The Nuage Networks NSG supports multiple WAN uplinks.



2. To avoid link under-utilization, it is important for the CPE to be able distribute traffic across multiple uplinks.

   Nuage Networks VSP leverages application-aware routing (AAR) to dynamically route different applications over different uplinks depending on their L7 signatures and link states. AAR leverages product capabilities such as application discovery, network performance measurement and intelligent path selection.

FIGURE 7. The NSG supports application-aware routing (AAR).



PCI DSS compliance

The payment processing value chain is undergoing rapid transformation with the proliferation of transactions beyond the typical brick-and-mortar PoS. Banks and merchants that process payments are adopting cloud-based infrastructures to adapt their operations to these changes. While the underlying networking and compute infrastructure evolves, banks and merchants must ensure the security and integrity of consumer data by conforming to standards established by the PCI Security Standards Council.

The PCI DSS are the key standards established by the council for technical and operational system components included in or connected to cardholder data. Endorsed by major credit card companies worldwide, PCI DSS require merchants and service providers that store, process or transmit cardholder data to adopt information security controls and processes to ensure cardholder data is protected.

TekSecure Labs, a leading provider of technology risk management services, is certified by the PCI Security Standards Council to validate compliance with PCI standards. TekSecure Labs has completed an audit of the Nuage Networks platform to test conformance to PCI DSS requirements. It concluded that Nuage Networks SDN and security solutions for cloud, datacenter and branch networks make it easier for organizations to achieve PCI compliance. Furthermore, there were no known limitations within the Nuage Networks solution components that might inhibit an organization's ability to become PCI-compliant, or maintain its existing compliance.

End-to-end security micro-segmentation

For retail network security, the Nuage Networks VSP leverages its VRS module and NSG to enforce micro-segmentation mechanisms end to end — from the branch store to the datacenter and public cloud. This ability to create end-to-end micro-segments ensures that all assets and user data are secure from unapproved access and malware lateral movement.

In addition, Nuage Networks VSP integrates with a series of firewall vendors (e.g., Checkpoint, Palo Alto, Fortinet). This enables customers to easily use advanced security solutions to enforce security remotely in a CO/POP or data-center location, as well as using cloud-based security such as Zscaler or Palo Alto Networks Global Cloud Protect.

As shown above, the security mechanisms in Nuage Networks VSP are implemented in the form of security policies attached to domain templates. Once created, these can be instantiated as many times as needed, making retail chains ideal candidates for this type of design.

Optimum application performance

Providing wireless in-store access to shoppers is definitely a "must-have" feature today. This is just one of the ways in which physical retailers are embracing the digital world. However, this comes at a price. One needs to make sure that the guest Wi-Fi will not impact other important traffic, like Voice over IP (VoIP) and business-critical applications.

In addition to the security capabilities and the ability to isolate traffic, the VSP provides quality of service (QoS) mechanisms that enable the classification and limitation of network traffic. This can help prioritize critical traffic, such as VoIP, over the non-critical, such as customer Wi-Fi, which will be sent in best-effort mode.

Furthermore, AAR can help optimize egress traffic flow. Using L7 application signatures and link occupancy rates, the solution can dynamically distribute the traffic across two WAN uplinks (internet and MPLS, for example).

This combination of QoS and AAR makes end-to-end traffic optimization and control not only possible, but simple.

Full network visibility

One of the most difficult aspects of troubleshooting network issues is the lack of visibility. Most traditional networking vendors do not put enough emphasis on the monitoring and visibility capabilities of their solutions.

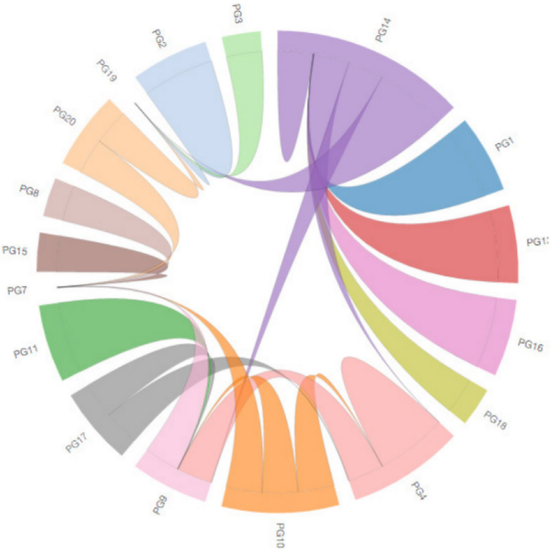
The Nuage Networks VSS is a software-defined security service for datacenters and wide area network (WAN) environments. It runs on the Nuage Networks VSP and helps address protection, detection and operational security challenges in cloud environments, including emerging security threats and multi-tenancy. VSS is the industry's first distributed, end-to-end (cloud, datacenter and branch), SDN-based security, visibility and automation solution. Running on Nuage Networks VSP, also an SDN platform, VSS adds security capabilities that provide contextual traffic visibility and security monitoring, as well as dynamic security automation for rapid incident response. Combined with the inherent VSP capabilities, such as micro-segmentation, policy automation and policy enforcement, VSS delivers visibility, analytics and dynamic threat response.

The Nuage Networks VSP security follows a three-pronged security methodology with separate components and features to address each step in the security lifecycle:

1. Prevent security incidents by minimizing the attack surface with software-defined micro-segmentation and policy enforcement across the cloud, datacenter and WAN
2. Detect security threats and monitor compliance with contextual network visibility and security analytics in real-time
3. Respond faster to security incidents and breaches by automating remediation processes such as quarantining suspicious applications or engaging deeper analysis tools.

For compliance validation, network security administrators and auditors can visualize traffic flows with context (e.g., policy group and domain) both within and between datacenters and branch stores. In addition, they can audit and define whitelist security policies for micro-segmentation using application flow mapping. Based on contextual flow visualization, the VSP can, for example, map L4 protocol/ports information used by flows between application components or policy groups.

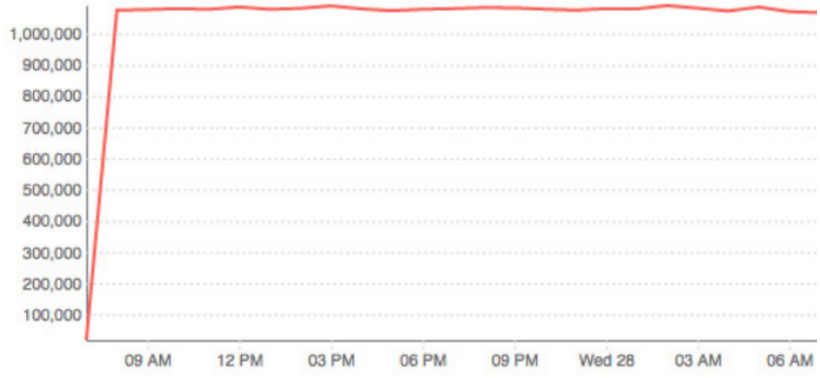
FIGURE 8. Contextual flow visualization of ports and protocols with the Nuage Networks VSP.



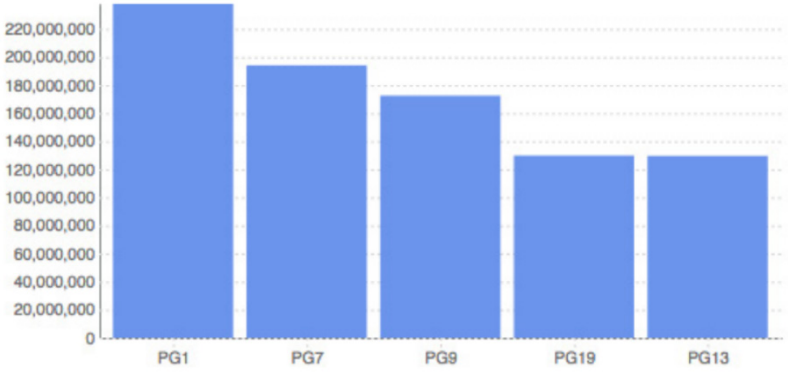
Network security and operations teams can get insight into network security events with near real-time security alerts, security dashboards and reports based on traffic analytics as well as ACL-allow/deny hits and security events.

Examples of security reports include:

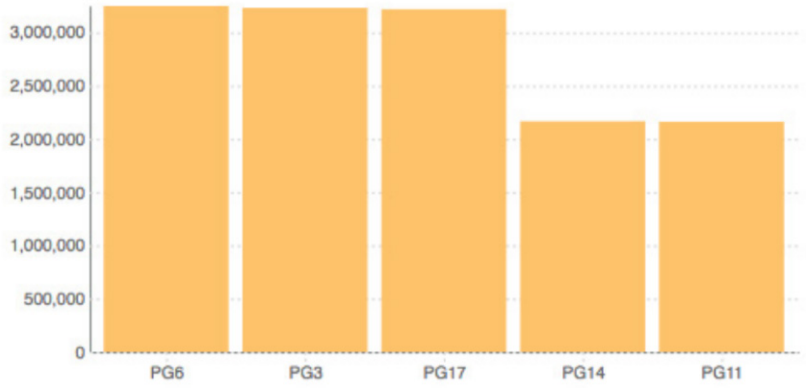
- ACL deny/allow count vs. time within a domain or the entire enterprise



- Security events by source/destination policy groups, or within a domain



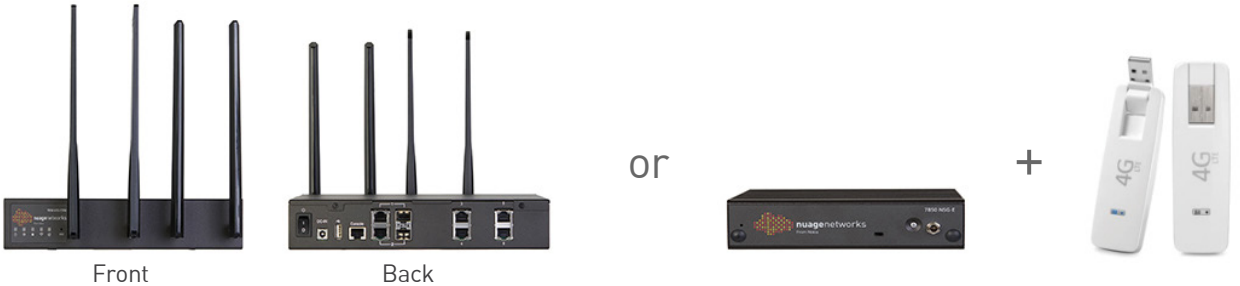
- Top source policy groups causing ACL denies within a domain.



Simple, flexible and highly automated site turn-up

Usually when a new branch store is set up, a significant amount of time is spent provisioning WAN circuits. Internet service providers (ISPs) can take 8 – 12 weeks to provision an MPLS circuit. As an interim solution, the NSG supports 4G/LTE connectivity out of the box. This way, the branch store can start operating using the LTE connection and when the MPLS and internet circuits are ready, they can be added without traffic disruption. The Nuage Networks LTE support has two options, embedded using the NSG E200/300 series devices, or using a USB LTE stick with any mode.

FIGURE 9. Two options, embedded and USB stick, for LTE support on the Nuage Networks NSG.



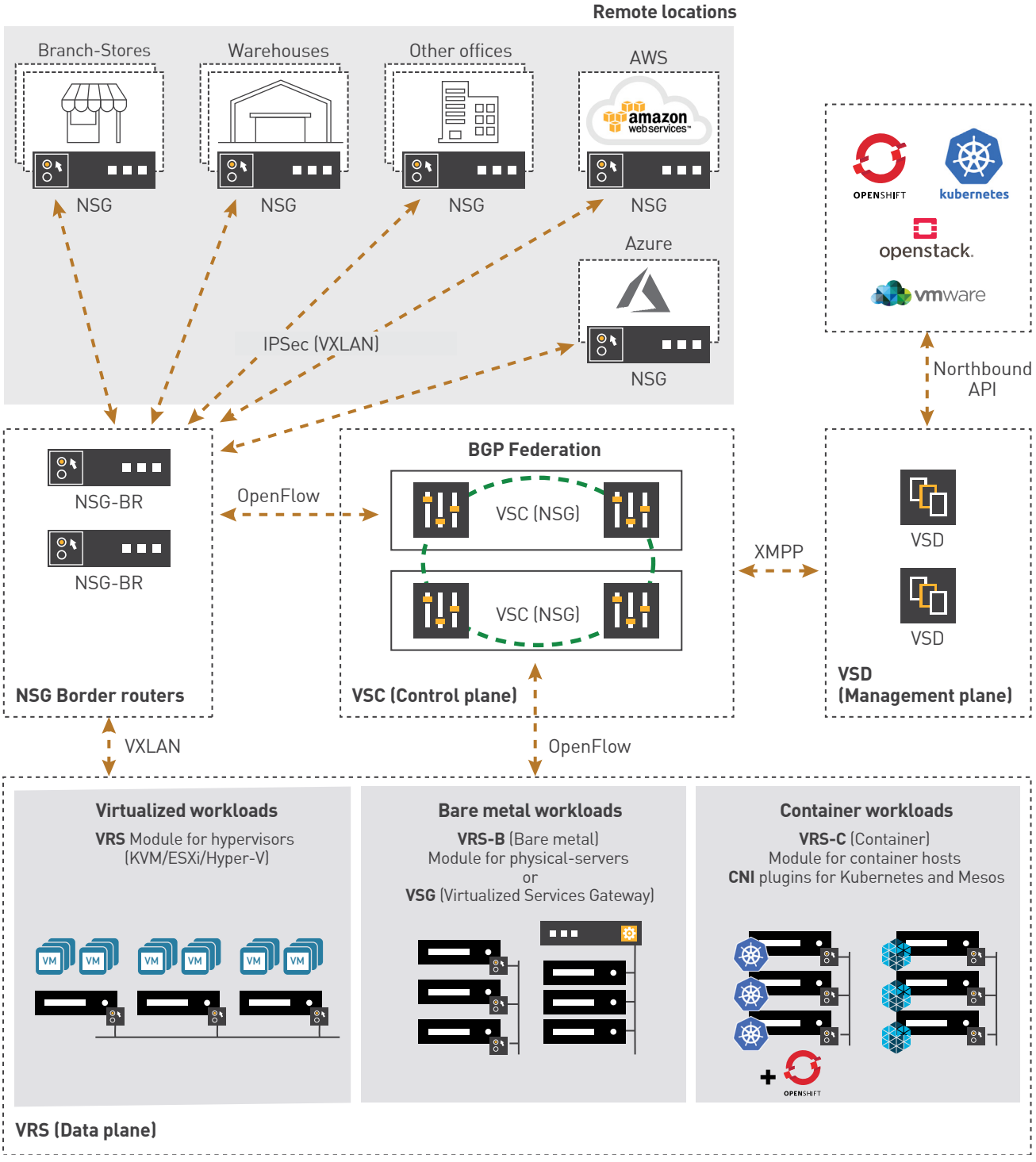
Front Back

7850 NSG-E206/306

Retail network design using Nuage Networks VSP

Having seen how Nuage Networks can help retail chains address their network and security issues, we will now discuss how to build today's retail networks using the Nuage Networks VSP. The diagram below shows some of the architectural aspects of the Nuage Networks VSP deployment.

FIGURE 10. Some of the architectural aspects of the Nuage Networks VSP deployment.



VRS (data plane) in the datacenter

Starting from the bottom of the diagram in figure 10, the VRS (data plane) block shows the different kinds of workloads supported. The Nuage Networks VSP supports all types of workloads available today, including:

Virtual machines (KVM, ESXi and Hyper-V)

The VRS data-plane module is installed on the hypervisor[1] and provides connectivity to the VMs. It supports KVM, VMware ESXi and Hyper-V.

Bare-metal servers

There are two ways of connecting bare-metal servers. The first uses a VRS-B (bare-metal) module, which is installed in the bare-metal servers operating system (RHEL and Ubuntu are supported). The second uses a VSG to bridge bare-metal workloads to the Nuage Networks VSP virtual domain. This option doesn't require any installation inside the OS of the server. Depending on the amount of traffic to be processed, several VSG form-factors are available (virtual, small, medium and large).

Containers

Nuage Networks VSP supports a vast variety of container workloads from simple Docker containers to container orchestration services. A CNI plugin is available for independent Docker containers, and a CNM plugin can be used for Kubernetes and Mesosphere container orchestration services.

VSC (control plane)

All data-plane modules (VRS) are piloted by the VSC (control plane) block using the OpenFlow protocol. The design has two VSC groups: one to pilot the VRS modules; the other to pilot the remote NSGs.

All VSCs are in a BGP federation and share the same reachability information for all virtual tunnel end-points (VTEPs). Forming a BGP federation allows them to scale almost indefinitely; you simply add pairs of VSC as you add more end-points. The main role of the VSCs is to translate VSD policy rules into OpenFlow forwarding instructions for the VRS modules.

VSD (management plane)

The Nuage Networks VSD block is used to define the network topology, enforce security policies and also provides a northbound API interface to communicate with leading Cloud Management Systems (CMS). It is also the central configuration point for the cloud and tenant administrators.

NSG border routers (data plane) in the branches

The border router (BR) is a specific NSG function that is used to provide connectivity between the WAN and DC underlays. More specifically it does IPSec to VXLAN and VXLAN to VXLAN conversion for the data path. This will be the entry point for all remote locations that use NSGs.

Remote locations

On premises (physical) and public cloud (virtual) connection of remote locations are both supported. On-premises can be connected using a broad range of NSGs. Depending on the bandwidth requirements, one can use a virtual gateway (several hundreds of Mbps) or physical (10 Gbps). Public-cloud is available as an Amazon machine image (AMI), it can be used to connect AWS VPC to the private datacenter using secure IPSec communications. The Azure NSG image is currently being developed and will be available in the Nuage Networks VSP, release 5.4.1.

All NSG appliances have multiple uplinks and can be used with multiple WAN links simultaneously.

1 ESXi implementation is different. The VRS module is installed as a VM and traffic is routed through it.

Third-party VNF on NSG

The NSG supports the hosting of third-party VNFs to provide branch-in-a-box functionality through the integration of network appliances. The VSD manages the onboarding, deployment, datapath integration and life-cycle aspects of VNFs hosted on the NSG. Setup, configuration and deletion can all be handled using the VSD.

This can come in handy in branches, where local services like firewalls, proxies or WAN optimization are used. It avoids building an infrastructure to host dedicated hardware. Instead the virtualized network functions (VNFs) can be deployed on the x86-based NSG and integrated into the network path transparently using Nuage Networks VSP redirection policies.

Figure 11 shows how the access network traffic on an NSG can be service-chained through a succession of VNFs, then forwarded to one of the uplinks (MPLS or internet).

FIGURE 11. An example branch in a box using universal CPE to host various VNFs.

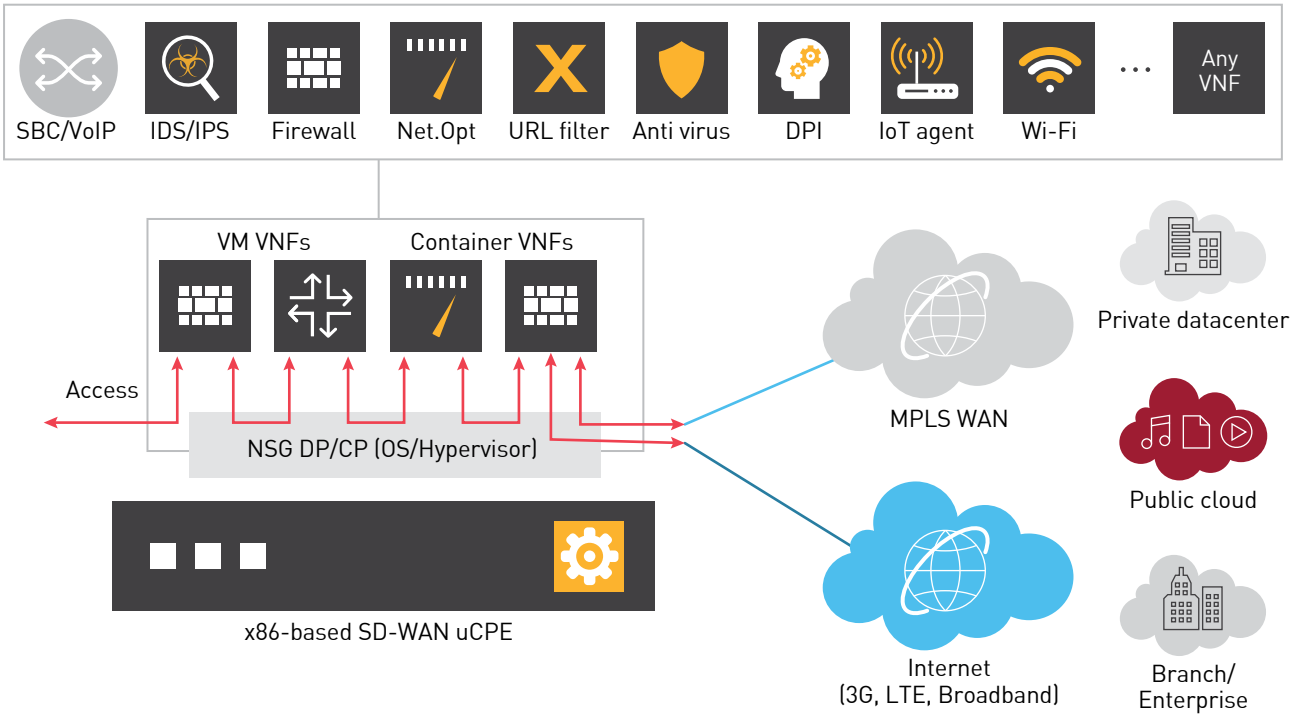
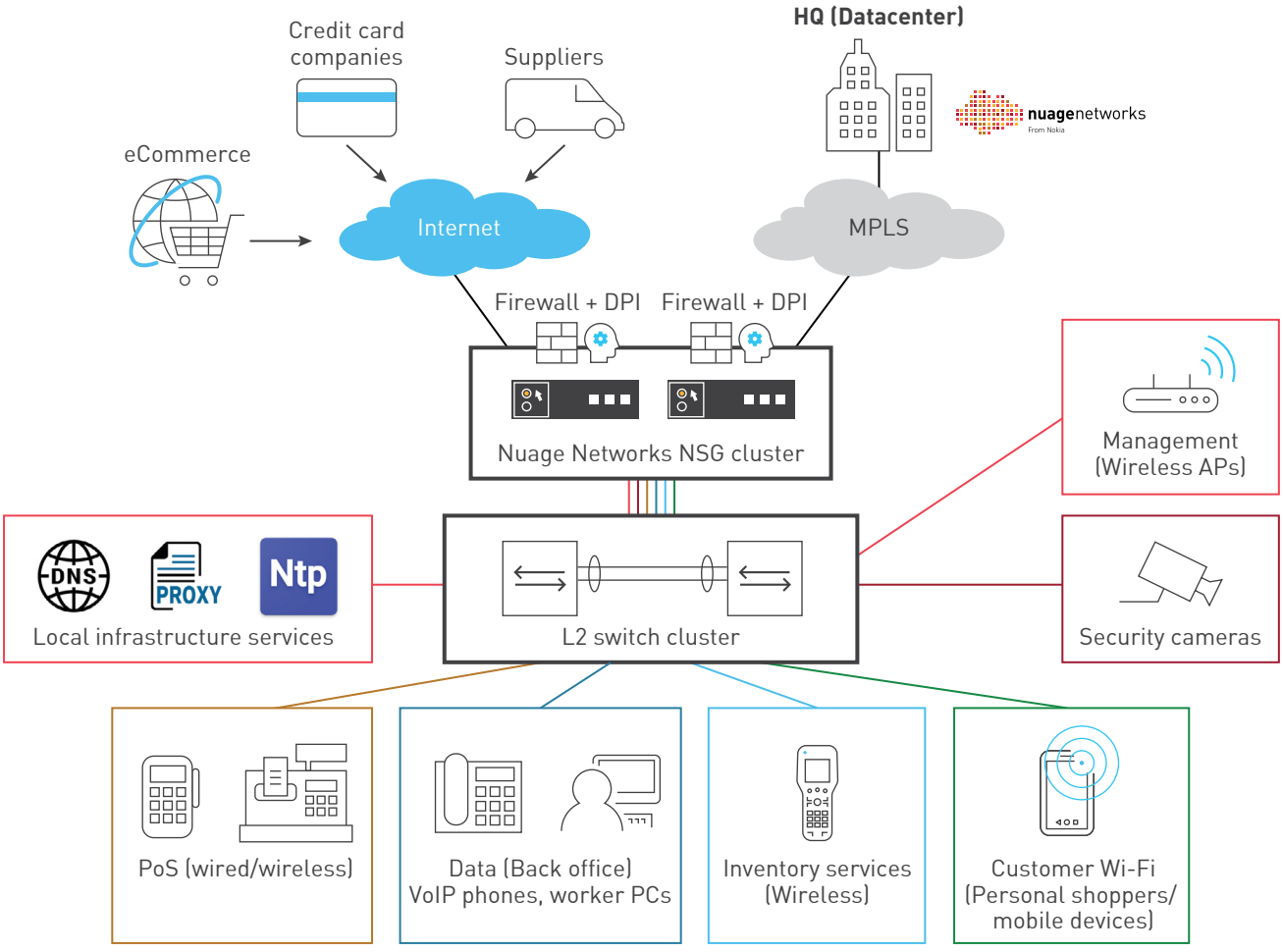


Figure 12 shows a slightly modified branch store network architecture which uses a cluster of Nuage Networks NSGs as CPE devices. They also host a firewall and DPI VNF, which will be inserted into the network data path and used to filter traffic dynamically based on the defined security/redirection policy.

We may see that the L2 switch cluster is still not involved in the routing process, passing the VLAN tags to the upstream CPE. Next the NSGs, based on the VLAN tags and input ports match the traffic and "decide" on the egress uplink and redirection policy to apply.

FIGURE 12: A slightly modified branch store network architecture that uses a cluster of Nuage Networks NSGs as CPE devices.



This design has several advantages, compared to the legacy design:

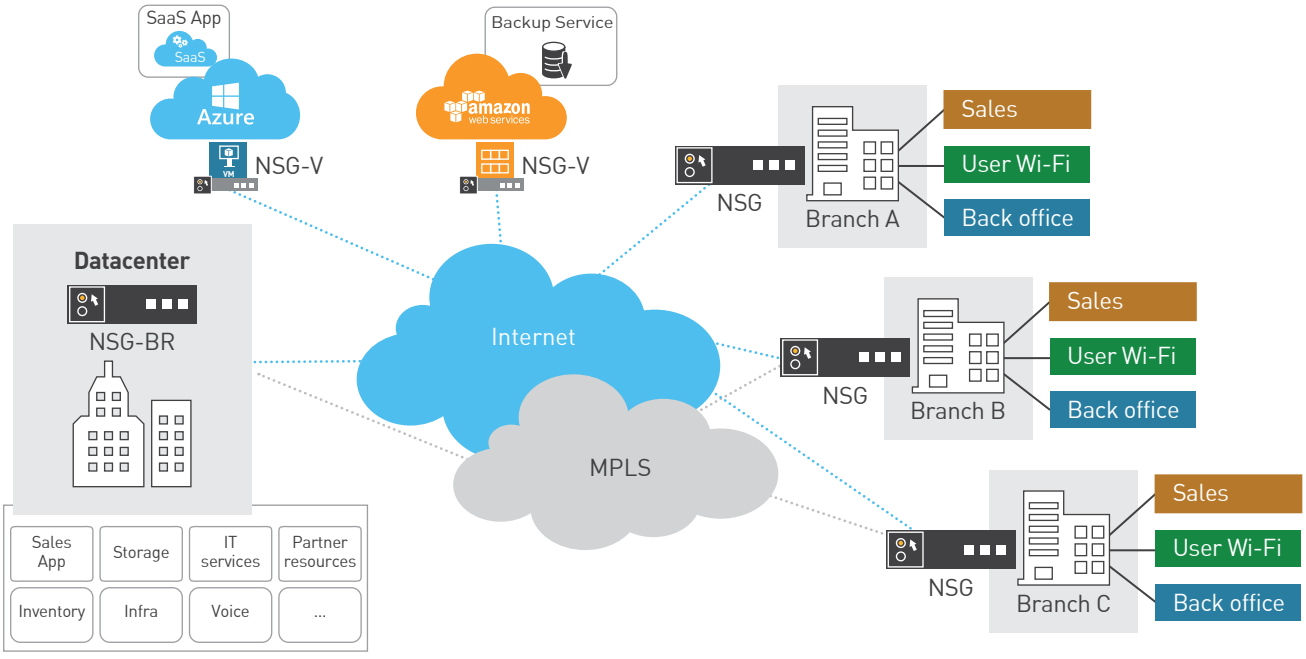
- **Automation –** The centralized management and control planes make it possible to configure and manage the network centrally using policies. Each configuration change can be pushed dynamically to all endpoints by modifying the template.
- **Openness –** Ability to host a wide range of third-party value-added services and functions that can be hosted on x86 uCPE.
- **Self-contained VNF management –** Lightweight LCM appliances are part of the Nuage Networks offer; it does not require additional management or orchestration systems. If desired, complex LCM schemes can co-exist and be implemented outside of the SD-WAN system.
- **Secure and tamper-proof operation: –** The Nuage Networks SD-WAN includes a secure, authenticated message channel between cloud policy plane and branch device. The channel is used for device bootstrapping, pushing policy/forwarding updates and extracting SD-WAN analytics data. The Nuage Networks "branch-in-a-box" utilizes the same channel for both VAS appliance bootstrapping and LCM, thereby ensuring fully secure, tamper-proof and encrypted operations.
- **Traffic monitoring and insight –** In order to derive full benefit from SDN-based automation for VAS, the system must provide pan-network flow/traffic analytics that are easy to consume via APIs and built-in visualization. The flow data can be used to automate the creation of policies based on real-time traffic, thereby dictating service chaining, mirroring and shaping for VAS traffic.

A sample network design using Nuage Networks SD-WAN

Figure 13 features a sample architecture for a retail chain showing, from left to right:

- The main datacenter containing all applications and resources used by the whole retail business group
- A couple of public sites (Azure and AWS) providing access to some SaaS (Software-as-a-Service) applications
- Several store locations (Branch A–C), containing different subsystems: backoffice, user Wi-Fi, and sales. For simplicity, only three branches have been depicted on this diagram.

FIGURE 13. A sample architecture for a retail chain built using Nuage Networks VSP constructs.

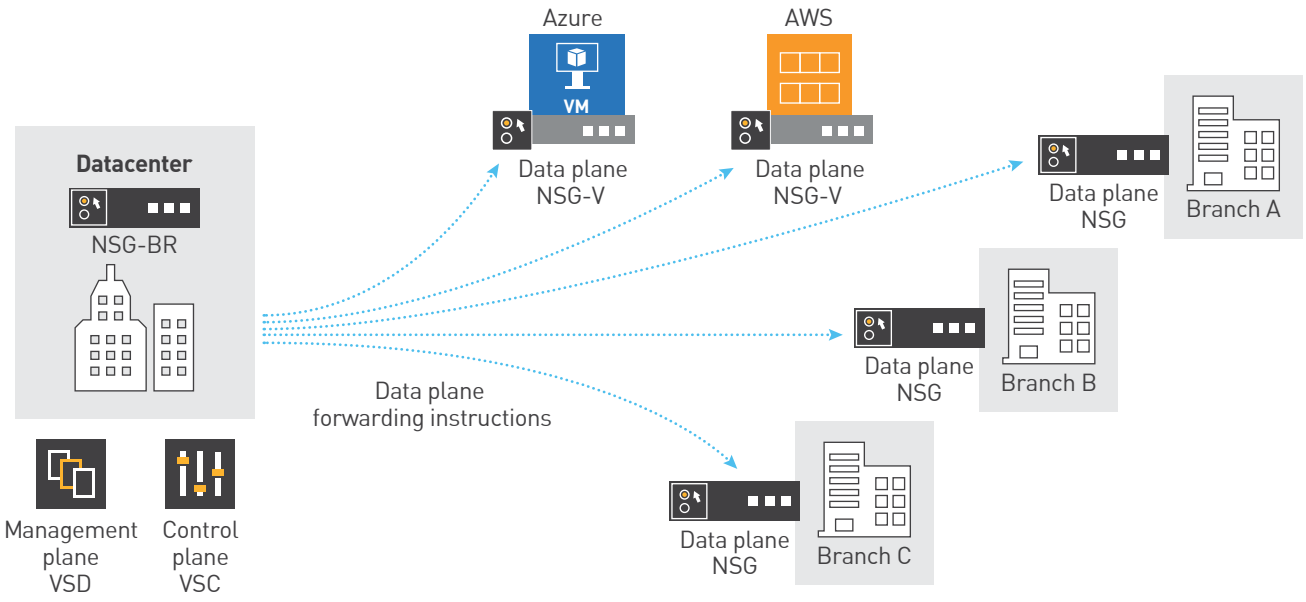


Depending on the availability and requirements, all locations listed above are connected either to the internet or to the internet and MPLS networks. The full-mesh secure connectivity between all sites in the diagram is set up by the CPE devices, which create encrypted point-to-point tunnels.

The diagram has been greatly simplified. However, in a typical design, there are multiple datacenters (active/active or active/passive), backup sites and hundreds (or even thousands) of branch stores.

This design enables the use of multiple WAN connection types. Again, for simplicity, only internet and MPLS have been shown, but the CPE devices support multiple active/active or active/passive uplinks.

FIGURE 14. Centralized management and control of the retail chain network.



This design allows centralized management and control of the whole network infrastructure. By placing the management and control plane components in a central location, every data-plane component and change in network behavior can be dynamically configured based on the state of the network.

Conclusion

In this document, we have described a typical retail chain IT architecture and explored the main technical challenges that the retail industry is facing in digital business transformation. Most retail networks are currently configured to handle neither the technical requirements nor the operational challenges. Fortunately, SD-WAN solutions do exist that can dramatically simplify the management of networks of hundreds and even thousands of branch stores using software tools that simplify setup and automate provisioning.

There is no question that retailers need to transform the in-store shopping experience. eCommerce has moved the goalposts and customers have come to expect more. Using digital technologies, retailers can enhance and augment how shoppers interact with their brands, blending the online and in-store, creating an omnichannel customer experience. In this paper we have looked closely at how the Nuage Networks SD-WAN 2.0 solution can help retail chains to meet these new challenges and cost-effectively and efficiently support the new connected-shopper experience.

Appendix A – Nuage Networks NSG overview

The Nuage Networks Network Services Gateway (NSG) can have several personalities. Depending on the connectivity use cases, it may act as simple provider edge (PE) equipment, as a border router (BR) or underlay border router (UBR). This section of the document will focus on explaining the purpose of each personality, as well as the associated use-cases.

Network services gateway (NSG)

The NSG is essentially provider-edge equipment installed at the remote location. Its role is to provide connectivity for branch devices and service demarcation between the branch and the WAN. Being based on the x86 COTS hardware, it can also host virtualized network functions (VNFs).

FIGURE 15. A traditional branch network consisting of back office, sales and user Wi-Fi.

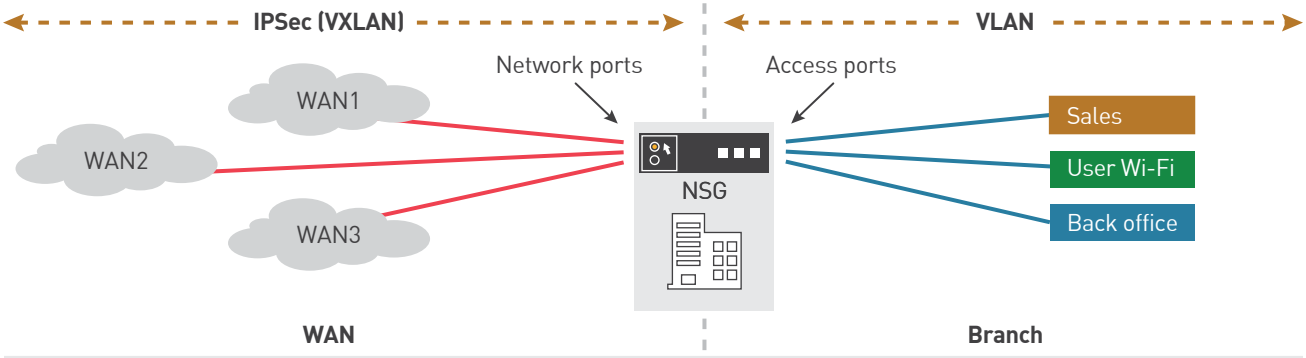
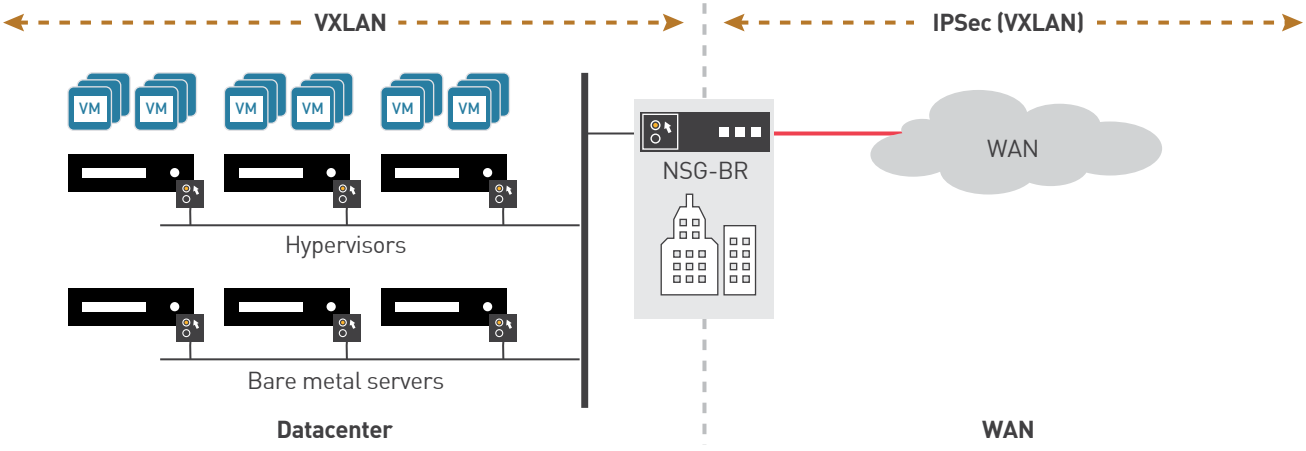


Figure 15 shows, on the right side, the traditional branch network consisting of the back office, sales and user Wi-Fi devices. These are connected to the traditional network, optionally using VLAN segmentation. The branch traffic comes in through the access ports of the NSG and is encapsulated into VXLAN and (optionally) IPSec before it is sent to the WAN network ports. Thus, the NSG acts as gateway for the branch store devices into the corporate network.

NSG border router (NSG-BR)

The NSG-BR is a different personality that provides a secure demarcation point between the WAN and data-center networks. It is used to terminate the WAN IPSec tunnels and provide connectivity to data-center workloads.

FIGURE 16. The NSG functioning as a border router to enable WAN connections for branch stores.

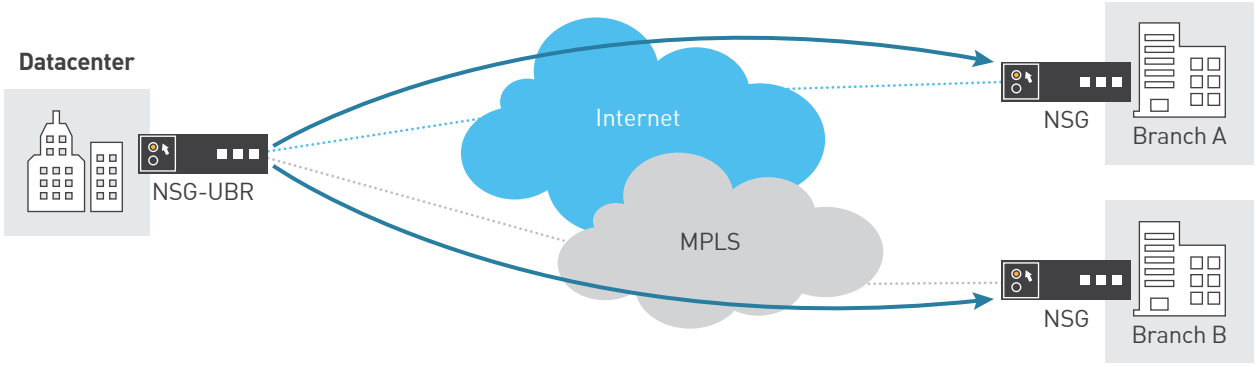


The NSG-BR is usually installed in the datacenter and acts as a BR for WAN connections from the branch NSGs. It terminates any IPSec tunnels from the untrusted WAN underlays and handles the connections to the datacenter.

NSG underlay border router (NSG-UBR)

The NSG-UBR is similar to the NSG-BR, but with the exception that it can provide seamless connectivity between multiple NSGs in disjointed underlay networks.

FIGURE 17. The NSG-BR offering connectivity either through the internet or an MPLS underlay network.



In cases where the remote locations are connected to different underlays, such as internet and MPLS as pictured in figure 17, the NSG-UBR enables them to communicate seamlessly, by creating one common, contiguous overlay network. It is usually installed in the datacenter and acts as a border router.

Document code: SR1901031732EN (January) CID202287