SDWAN

EANTC Independent Test Report

Nuage Networks SD-WAN 2.0 Solution

September 2018

EANTC

nuagenetworks
From Nokia

Introduction

Nuage Networks, a Nokia business, commissioned EANTC to conduct an independent test of the vendor's SD-WAN solution. The tests were executed at Nuage Networks headquarters in Mountain View, California, in August 2018.

At EANTC, we have continuously expanded our SD-WAN master test plan since 2016. It covers many aspects of the technology; typically vendors select a subset for which they are best prepared. Nuage Networks, in contrast, boldly selected all of them:

- Tenant and Location Scalability
- Multi-Tenancy Management
- Endpoint and Link Resiliency
- Performance Monitoring
- Service Chaining & Elasticity

By investigating all these areas in the course of three weeks of testing (one week remote and two weeks on site), the EANTC team was able to analyze the solution in detail. Specifically the broad range of scalability and functionality tests helped to get a good grip on the Nuage Networks SD-WAN 2.0 solution's readiness: We verified its support for very large tenants and for a huge number of small tenants; we tested full-mesh tunnels at max, each carrying traffic; we investigated multiple types of physical and virtual CPEs. The service scale results were flawless and matched the vendor's claims.

The agility and resilience of the solution surpassed our expectations easily. Obviously, Nuage Networks has managed to combine extensive experience in service provider IP/MPLS transport solutions with SDN orchestration and service management knowledge. The connectionless tunneling solution is an innovative and well-functioning design.

We confirmed operational aspects such as the ability to add a new service to a multi-tenant CPE without impacting actual running services.

The Endpoint and Link Resiliency tests included CPE failure as well as the failure of one of the primary links. This showed that the SD-WAN solution is able to mitigate a failure and can maintain active services to the other branches.

Performance monitoring is one of the key enablers of SD-WAN. Link performance is optimized with the goal of finding the best path. Nuage Networks successfully demonstrated the performance monitoring features of the solution.

Test Highlights

- ➔ Scaling tested up to 4,000[a] virtual branches (NSGs) controlled by 20 Virtualized Services Controllers (VSCs), establishing up to 396,000 overlay tunnels across 40 tenants.
- ➔ Validated up to 129,240 full mesh overlay tunnels on a tenant[b] with 360 sites.
- ➔ Manages up to a tested 40 tenants[b] at a multi-tenant CPE
- ➔ Supports controller and site redundancy without single point of failure
- ➔ Implements CLI- and GUI-based performance monitoring
- ➔ Provides Zero Touch CPE provisioning and in-service tenant[b] creation
- ➔ Supports network service chaining functions

a. The scaling test limit was set at 4000 due to limited resources (servers).
b. Each tenant was created by a separate VRF.

All test configurations and results are described in detail in this report; EANTC's goal is to provide sufficient detail to enable reproducibility of results. In case of doubt, we are ready to answer questions at any time.

Hardware and Software

System under Test (SUT)	Version
Virtualized Services Directory (VSD)	5.2.3
Virtualized Services Controller (VSC)	5.2.3
Virtualized Network Services Gateway (NSG-V)	5.2.3
Physical Network Services Gateway (NSG-X)	5.2.3

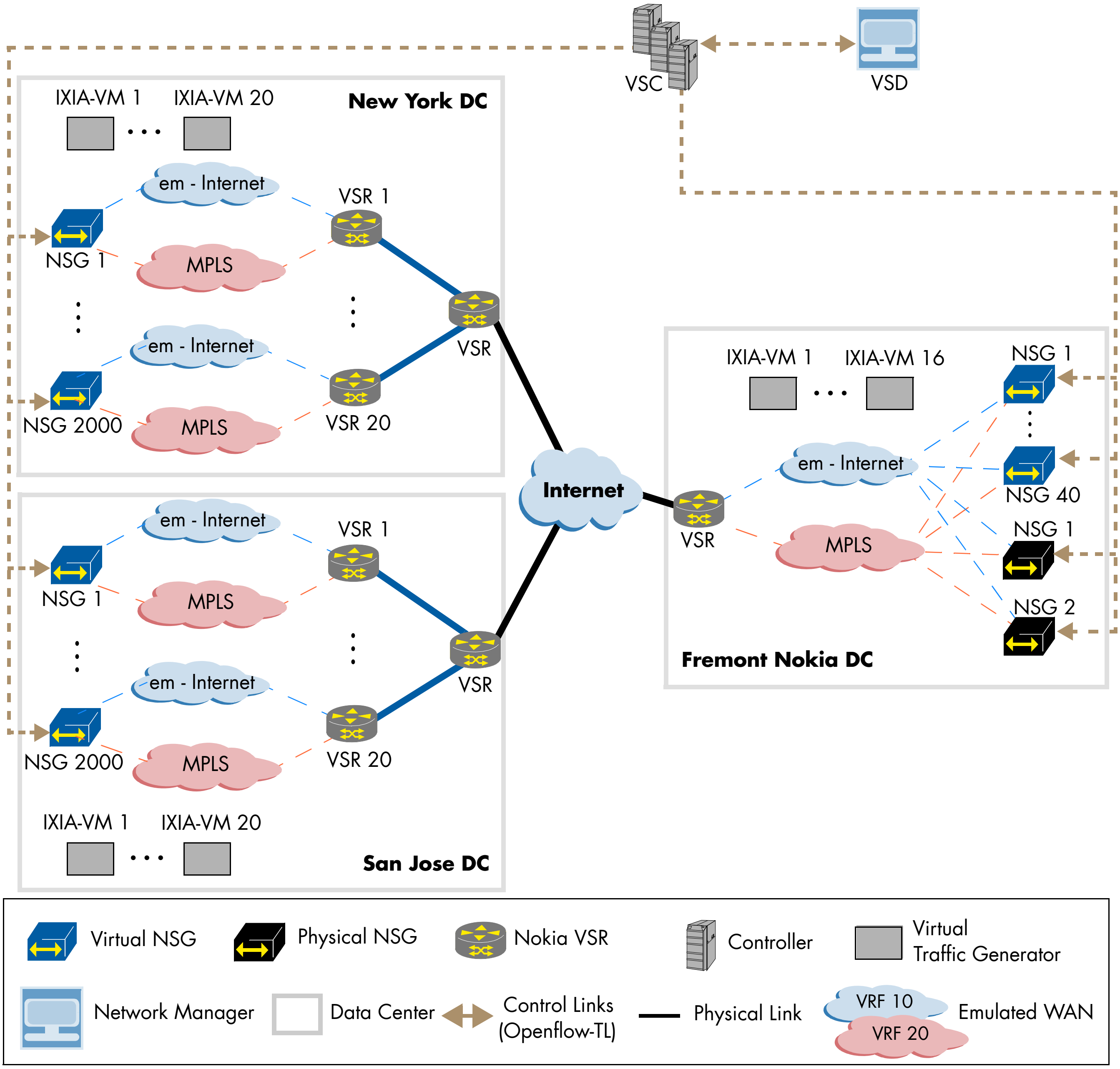

Figure 1: Test Setup

Test Bed

The Nuage Networks SD-WAN 2.0 solution consists of two major parts: The Virtualized Services Platform (VSP) and the Network Services Gateway (NSG). The VSP, in turn, has two main components: The Virtualized Service Directory (VSD) and the Virtualized Service Controller (VSC). VSD is a policy and business logic engine that is used to outline the networking requirements of the cloud applications. At the same time, VSC maintains the full view of network and service topologies and instantiates network service templates defined through the VSD. NSG is the Customer Premises Equipment (CPE) which is the endpoint of a network service.

Nuage Networks provided a comprehensive end-to-end lab environment for the test. The test bed consisted of three Data Centers (DC).

They were located in New York, San Jose, and Fremont. In the New York DC, 2000 virtual NSGs were instantiated and every 100 NSGs were connected with one Nokia Virtual Service Router (VSR) instance. The VSR is not part of the Nuage Networks SD-WAN 2.0 solution and was used in this test to replicate the WAN underlay networks (MPLS and Internet). Each VSR was able to manage the Internet and MPLS traffic with two different VRFs. In total, 20 VSRs were instantiated in the New York DC to connect all 2000 NSGs. An additional Nokia VSR was used to connect all 20 VSRs and passed the traffic to an external link. Each NSG was managed by two VSCs and a total of 10 distributed VSCs controlled all 2000 NSGs in the DC. 20 IXIA VMs were deployed in the DC and connected with each NSG via different VLANs. San Jose DC was configured with the same setup as the New York DC.

In the Fremont DC, 40 virtual NSGs and two physical NSGs were installed. A single Nokia VSR was used to connect all the NSGs. Two VSCs were used to control the 42 NSGs. 16 IXIA VMs were deployed in the DC and connected with each NSG via different VLANs. All three DCs were connected by public Internet.

The entire test bed was managed by a single VSD which facilitates the graphical user interface to control and design the overlay network.

Test Equipment

For the test execution, we employed virtual traffic generators with 56 virtual components and two types of applications. IxNetwork (8.40) was used for L2/L3 traffic and IxLoad (8.40) was used for L7traffic. As the impairment tool, we had two Ixia Anue CKL-2U H Series Hawaii.

Scalability

Enterprises and service providers are particularly interested in the scalability of an SD-WAN solution. Through the following series of tests, EANTC verified various scalability claims of the Nuage Networks SD-WAN 2.0 solution, specifically:

- Number of Sites
- Number of VPNs
- Number of VPN per Tenant

All three test cases were performed with the virtual CPEs.

Number of Sites and Number of VPNs

As the SD-WAN solution is intended to be used by large organizations and enterprises to provide connection to thousands of distributed branch sites, the scalability of the solution in terms of number of sites and number of VPNs becomes an important factor in the deployment.

For the number of sites and number of VPNs test setups, Nuage Networks selected two data centers which are located in New York and San Jose. Each data center consists of 2000 virtual CPEs (NSG). Each NSG was connected with two virtual links in which one link was connected with the MPLS network and the other link was connected with the emulated Internet. Each link was used to connect with a single VSC and each NSG was managed by two VSCs. In total, 20 VSCs were used to manage 4000 NSGs in this setup. Between 20 VSCs and 4000 NSGs, 8000 OpenFlow-TLS (OF-TLS) sessions between the VSCs and the NSGs, used for control, were established in a full mesh. All the VSCs were managed by a single VSD. By using the VSD Architect user interface, we created 40 tenants and attached 100 NSGs per tenant. In Nuage Networks SD-WAN 2.0, each tenant is created by a separate VRF. Figure 2 describes a tenant level NSGs alignment.

To verify the establishment of the setup, we generated bidirectional Layer 3 traffic between the sites and the Headquarter (HQ) by using 40 IXIA virtual machines and IxNetwork. During the traffic flow, 7920 bidirectional VxLAN data tunnels were established. The performance monitoring was activated between the sites and HQ and there was no traffic loss observed during the test. Our results show that Nuage Networks can maintain 4000 NSGs with the current setup for an SD-WAN solution.

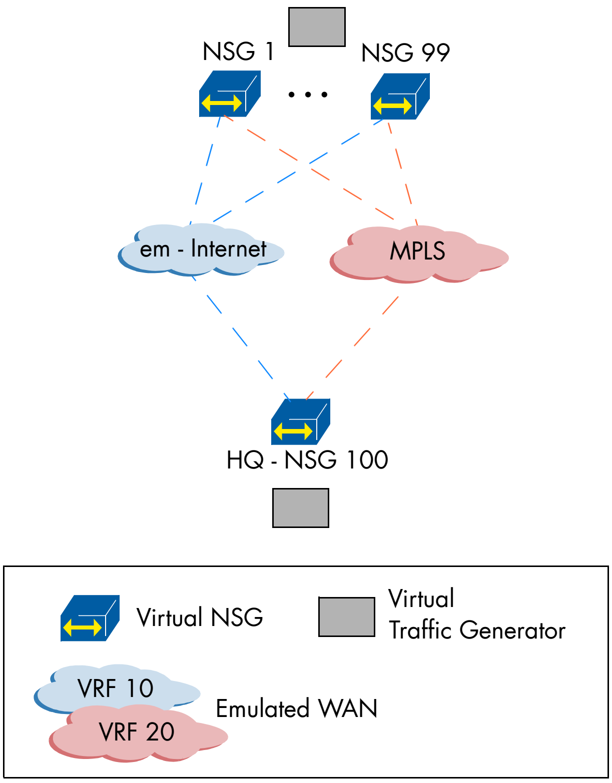

Figure 2: Tenant Level NSGs Alignment

Another important factor for an SD-WAN solution is the number of VPNs. It is essential for a solution to deploy, configure and manage a large number of overlay tunnels in a large scale deployment.

For this test setup, the policy was configured on all the CPEs by the controllers (VSC) to support full-mesh in the forwarding plane. In a full mesh network, overlay tunnels are required between all remote sites.

To verify the number of overlay tunnels, we generated a bidirectional Layer 3 traffic in a full mesh scenario. Each NSG in a tenant established two VxLAN tunnels (for both directions) with rest of the 99 NSGs in the same tenant. With 40 tenants and 4000 NSGs, Nuage Networks could successfully maintain 365,000 VxLAN tunnels without any traffic loss.

Number of VPNs per Tenant

In a large-scale multi-tenant SD-WAN deployment with a large number of branch sites per customer tenant, a single CPE device is often required to support a high number of overlay tunnels to enable connection to multiple sites.

In this test scenario, we added 360 NSGs to a single tenant by using the VSD Architect user interface. 10 VSCs are used to manage all the NSGs. Between 10 VSCs and 360 NSGs, 720 OpenFlow-TLS (OF-TLS) control sessions were established in full mesh. The NSGs are configured with the policies to connect all sites in the same tenant. Performance monitoring was activated between all the NSGs.

To verify the number of overlay tunnels per tenant, we generated bidirectional Layer 3 traffic in a full mesh scenario. Each NSG in a tenant established two VxLAN tunnels (for both directions) with remaining 359 NSGs in the tenant. In total 129,240 VxLAN overlay tunnels were successfully established by the SD-WAN solution within a tenant. Traffic was passed through the tunnels without any loss.

Multi-Tenancy Management

For service provider operating managed services, SD-WAN allows the creation of multiple separate business entities at a single SD-WAN device at the headquarter/data center by using network and security functions deployed on commodity servers. For this purpose, customer services are fully separated from each other by applying the concept of multi-tenancy.

The two major concerns in the multi-tenancy concept are add in-service customer tenant, and scalability of a tenant at CPE. We verified both abilities with the Nuage Networks SD-WAN 2.0 solution.

Add In-service Customer Tenant and Scalability of Tenants at CPE

In an SD-WAN solution, adding a new customer tenant (new service) to a multi-tenant SD-WAN CPE without impacting actual running services (in-service) is an important feature. In order to verify this capability in the Nuage Networks SD-WAN 2.0 solution, we performed the test in the Fremont Nokia data center.

By using the VSD Architect user interface, we created nine tenants and added a single virtual NSG to each tenant. At the same time, we created the nine tenants on the multi-tenant physical NSG. Two VSCs are used to control the NSGs. We generated bidirectional Layer 3 traffic between NSG and multi-tenant NSG and we observed zero packet loss. Each NSG in a tenant established two VxLAN tunnels (for both directions) with multi-tenant NSG. In total, 18 VxLAN overlay tunnels were established in the tenant. During the traffic flow, performance monitoring was activated between the NSG and the multi-tenant NSG.

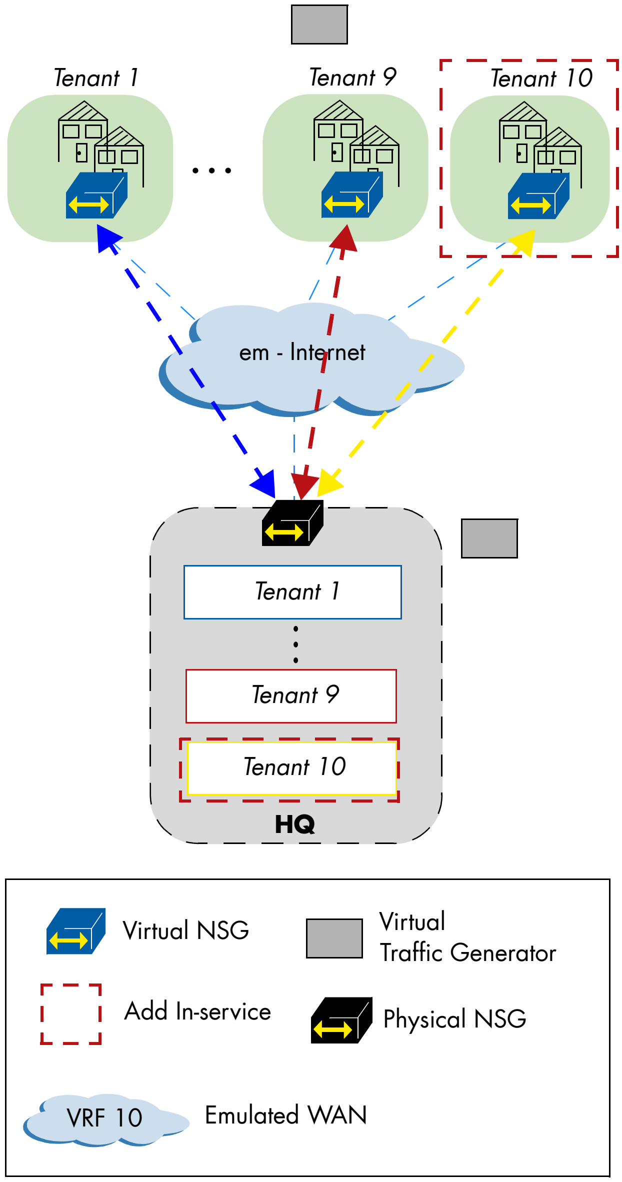

Figure 3: Add In-service Customer Tenant

While the traffic flow was established, we used the VSD Architect UI to create a new tenant in the multi-tenant NSG and connected a new CPE with the newly created tenant. While adding the new service, we observed no distraction in the traffic flow. We generated the additional traffic through the newly created tenant and after a few seconds, the traffic was successfully passed through the newly added NSG.

Scalability of Tenants at CPE

We used 40 virtual NSGs and one multi-tenant service activated physical NSG from the Fremont Nokia data center. In this test, Nuage Networks was interested to show the tenant scalability as 40 tenants at the multi-tenant NSG.

With the VSD Architect user interface, we created 40 tenants and added single virtual NSG to each tenant. The multi-tenant physical NSG was created with 40 tenants. The performance monitoring was activated between the NSG and multi-tenant NSG.

We generated the traffic for each tenant and observed zero packet loss. During the traffic flow, 40 VxLAN overlay tunnels were established in the 40 tenants. To verify the tenant isolation, we sent traffic in a full mesh configuration across all tenants and, as expected, we observed 100% traffic loss on the traffic flow between different tenants.

Nuage Networks successfully demonstrated 40 isolated tenants in the multi-tenant NSG.

Endpoint and Link Resiliency

Network reliability has always been a huge concern in any enterprise and service provider network while transporting voice, video, and business-critical data. Whether a link or a CPE fails, a reliable network should react to sudden failures without any manual intervention. The Nuage Networks SD-WAN 2.0 solution addresses such network failures.

Dual-Homed Services at the CPE Site

The ability to mitigate the failure of a critical component of the solution such as the CPE is crucial for some customer deployments. As the CPE is responsible for connecting the customer services to the other branches, the SD-WAN solution must be able to mitigate the failure of this component in order to maintain active services to the other branches. The active customers should remain completely stable and should be migrated to the (previously) passive CPE.

By using the VSD, we created a tenant. We added two physical NSGs and one virtual NSG into the tenant. All the NSGs are managed by two VSCs. In the VSD, a branch location is redundantly attached by two SD-WAN physical CPEs (NSG-X), each of which was connected to the remote device (virtual NSG-V) over an emulated Internet and an MPLS network. Both physical CPEs were configured to operate in master-backup redundancy mode and Nuage Networks configured Bidirectional Forwarding Detection (BFD) with a VLAN on the LAN side between both NSGs. All BFD sessions were used to monitor the connections.

Nuage Networks configured the BFD hello interval at 500 milliseconds. After a failure was detected, time for convergence is needed and this may take additional time.

We generated bidirectional Layer 3 traffic between the branch and remote device and a VxLAN overlay tunnel was established between master NSG-X and remote virtual NSG-V over the emulated Internet.

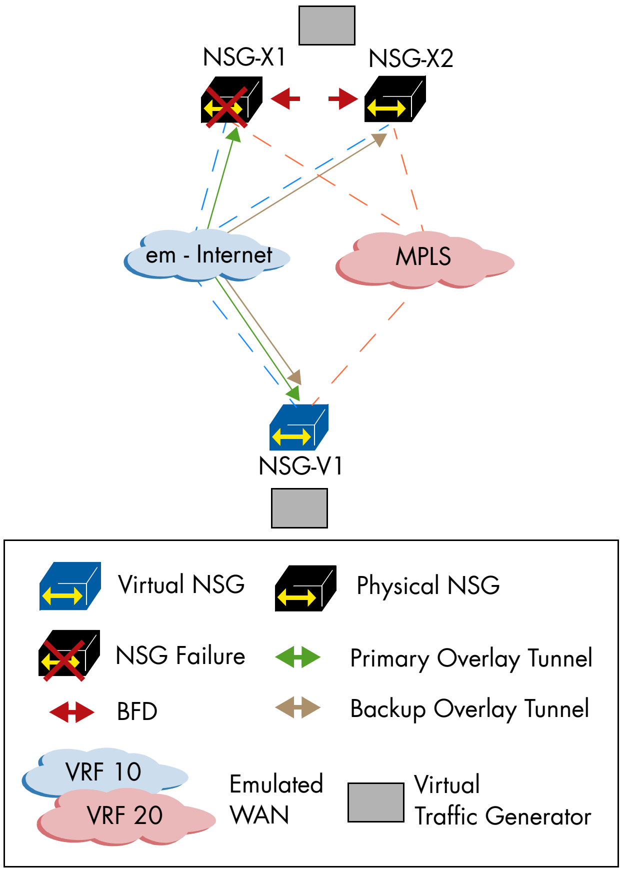

Figure 4: Dual-Homed Services at the CPE Site

Performance monitoring was activated between the branch and remote site.

While running the traffic, we emulated the failure of the master NSG-X by removing the power cable. The backup NSG-X became master and the traffic was redirected. We recorded an out of service time of maximum 4,644 milliseconds in the direction from the remote NSG-V to the branch NSG-X and a maximum of 1,704 milliseconds in the opposite direction. We reconnected the power cable of the failed NSG-X and tested the recovery scenario during the restart of the failed NSG-X. The previously turned off NSG-X became the master and the NSG-X who was previously the master became the backup. The traffic was steered towards the previously turned off NSG-X. We measured a recovery time of maximum 23,557 milliseconds in the direction from the remote NSG-V to the branch NSG-X. This delay was due to the control plane reconvergence. The maximum recovery time was 8,565 milliseconds in the opposite direction.

Nuage Networks successfully demonstrated the CPE failover and recovery maneuver with their SD-WAN 2.0 solution.

Primary CPE Uplink Failure

One of the key advantages of SD-WAN technology is the ability to aggregate different WAN links (such as MPLS, xDSL, LTE/4G). The ability of the SD-WAN solution to mitigate the failure of the primary link is critical.

In this setup, two physical CPEs (NSG-X) are attached to a single tenant by using the VSD. Each NSG-X was connected with two VSCs via MPLS and Internet network. Both NSG-X were connected together via two WANs (MPLS and an emulated Internet network). The traffic policies were provisioned to use the Internet link as primary and the MPLS link as a backup. The performance monitoring was activated via both links.

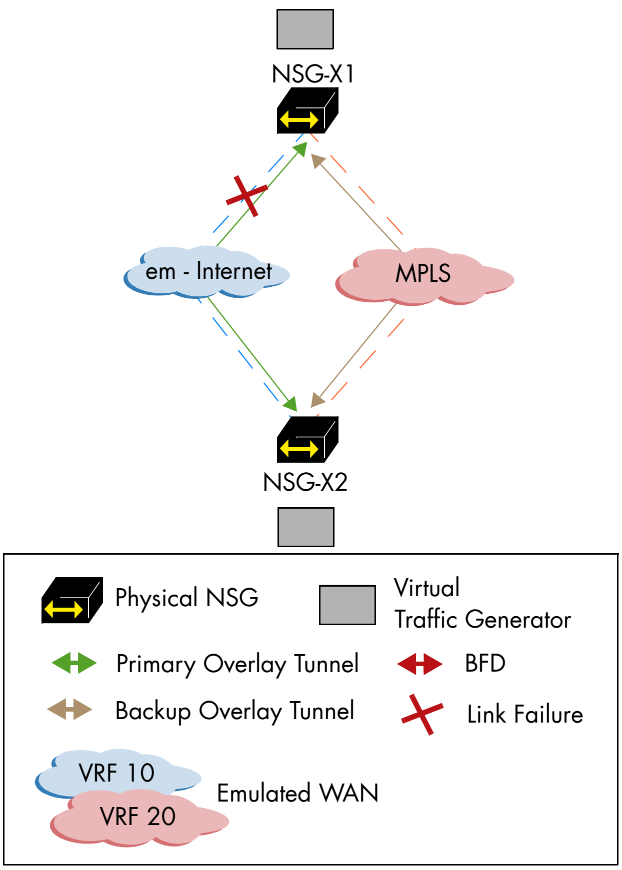

Figure 5: Primary CPE Uplink Failure

We generated bidirectional Layer 3 traffic by using IxNetwork. Traffic was steered towards the emulated Internet and zero packet loss was observed. A VxLAN tunnel was established towards the Internet network between both CPEs. While generating the traffic, we emulated a link failure between the NSG-X1 and emulated Internet by shutting down the port of the impairment device which was connected between the NSG-X1 and the emulated Internet. We successfully verified that traffic was redirected to the backup MPLS link as expected. The emulated Internet connectivity failure generated a failover time of 6,591 milliseconds in the NSG-X2 to NSG-X1 direction and 120 milliseconds in the opposite direction.

We also tested the recovery scenario by reconnecting the previously disconnected link via rebooting the port of the impairment device. As expected, the traffic was steered again towards the Internet link. We measured a recovery time of zero seconds. All test runs showed no traffic loss at all.

Accuracy of Performance Monitoring

The accurate measurement of performance metrics, such as packet loss and packet delay, is crucial to the correct operation of an SD-WAN-enabled network. This feature enables real-time visibility into the network which is key for application performance and reliability, the main drivers behind SD-WAN.

We used the same test setup as for the Primary CPE Uplink Failure test (see Figure 3).

The performance monitoring of overlay network connections between NSG-X is measured with a specific network profile (service class, payload size, and traffic rate) to find the path performance. In this test, Nuage Networks used UDP packets with a size of 137 Bytes and with a rate of 10 packets per second. The performance metric of the paths was updated by each NSG to the Elastic Search which is a database for collecting the statistics. During this procedure, the team used the Grafana application to visualize the performance of the network links which reported on packet loss, packet delay and jitter data collected by Nuage Networks Elastic Search.

We initially ran a baseline reference test without insertion of any impairment to validate performance monitoring implementation of the Nuage Networks SD-WAN 2.0 solution. For this purpose, we generated bidirectional Layer 3 traffic by using the IxNetwork. The traffic was steered towards the emulated Internet. We observed 0% packet loss in both directions, 0.614 milliseconds packet delay in the direction of NSG-X2 to NSG-X1 and zero milliseconds in the opposite direction.

For the packet loss measurement, we introduced 10% loss in the direction of NSG-X1 to NSG-X2 by using the impairment tool. We saw a range of 7.5% to 10.8% packet loss in the direction of NSG-X1 to NSG-X2 and 0% packet loss in the opposite direction. Nearly the same packet delay behavior was observed in the reference test. Once we removed the impairment profile, the loss value reverted to its normal condition.

In order to test packet delay measurement, we introduced an impairment that added a constant delay of 20 milliseconds to all packets on the Internet link in the direction of NSG-X1 to NSG-X2. A constant delay of 10 milliseconds was added to all packets on the Internet link in the opposite direction. We observed 19.92 milliseconds packet delay in the direction of NSG-X1 to NSG-X2 and 10.18 milliseconds in the opposite direction. Again, 0% packet loss was observed in both directions.

Service Chaining & Elasticity

With growing enterprises, value-added virtualized services and zero-touch provisioning have become an important concept for SD-WAN solutions.

Chaining Network Service Functions

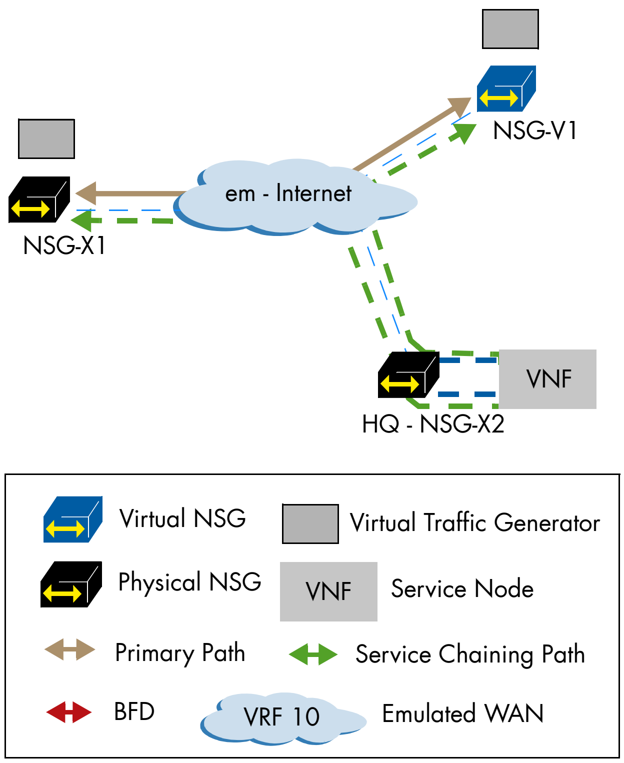

Figure 6: Service Chaining in HQ

In a data center or at a customer site, service nodes are deployed at various points in the network topology. These nodes provide a range of service functions which should not affect the currently running service. This test focused on the integration of a new virtual network function (VNF) into the current network service in a data center or within an SD-WAN solution.

Nuage Networks demonstrated two different test scenarios:

- Adding a new VNF to a headquarter (HQ)
- Adding a new VNF to a site

The two scenarios are depicted in Figure 6 and Figure 7. In the VSD, we created a tenant and added two physical NSGs (NSG-X1 and NSG-X2) and one virtual NSG (NSG-V1). NSG-X2 was set up as HQ and NSG-X1 was set up as a branch. Meanwhile, the NSG-V1 was created as another branch. For the second scenario, both physical NSGs were established as branches. A single VSC is used to control the NSGs in the tenant.

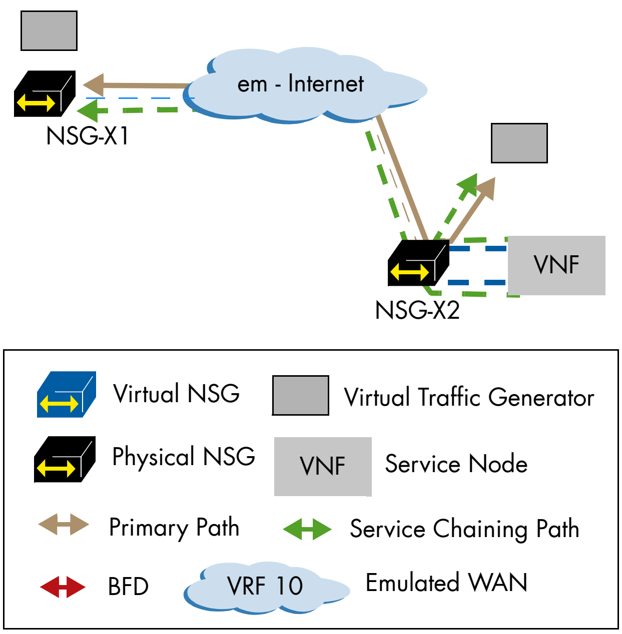

Figure 7: Service Chaining in Branch

For the first scenario (Adding VNF to an HQ) as in Figure 7, we generated the UDP traffic between two sites (NSG-X1 and NSG-V1) and observed zero packet loss. During the traffic flow, we added a generic firewall VNF to the HQ (NSG-X2) by using the VSD Architect user interface. In the network policy of the VSD, we created a service chaining including the new VNF to forward the traffic from NSG-X1 to NSG-V1 (NSG-X1 –> HQ (NSG-X2) –> VNF –> HQ (NSG-X2) –> NSG-V1). By using the IxLoad, we generated HTTP traffic through the newly created service chaining and zero packet loss was observed in the UDP as well as the HTTP traffic.

For the second scenario (Adding VNF to a site), we used two physical NSGs (NSG-X1 and NSG-X2) as remote sites and generated the same UDP traffic between the NSG-X1 and NSG-X2. We observed zero packet loss. We followed the same procedure for adding the new VNF with the NSG-X2 as described in the first scenario. We configured the new service chaining as NSG-X1 –> NSG-X2 –> VNF –> NSG-X2. We generated HTTP traffic through the newly created service chaining and observed zero packet loss for both traffic types.

During the traffic flow in both scenarios, we blocked the port 80 traffic in the added VNF and observed 100% packet loss for HTTP traffic and 0% traffic loss for UDP traffic.

Nuage Networks successfully demonstrated the value-added service for network service changing with their VNF, not only in the HQ but also at the site.

Zero-Touch Provisioning

Automating the provisioning of a new SD-WAN site is an essential tool to support any deployment regardless of branch scale. Automated provisioning enables customers to turn-up new sites, move/add/change WAN circuits or service configuration without requiring skilled personnel. Establishing an SD-WAN connection simply involves plugging in the CPE power and network cables.

Nuage Networks implements an automated bootstrapping architecture which enables the NSG end-points to securely connect to a VSP instance, pass authentication and authorization checks, download the service configuration (and any software updates required); and connect end-users to the network services based on pre-defined policies. As part of this provisioning automation, site/device/service configuration can be performed days or weeks in advance of the NSG attaching to the network, as well as performing a real-time modification to services after go-live.

The Auto-bootstrapping method tested provides a tool-free installation method for the on-site personnel by including VSP rendezvous data on a USB stick – which can be created in advance, or at the site during turn-up. The rendezvous data provides the NSG with the information to connect to the VSP instance and wait in a pending state, at which point the NSG must be assigned to an enterprise by the CSProot (VSP administrator). The enterprise administrator (or CSProot) can then authorize the NSG to the network; at which point the site/device/service configuration and any updates are pushed to the NSG.

Using the VSD, we created a tenant and added two physical NSGs to it. Both NSGs are connected with a single VSC and policies were configured to permit traffic flows to pass. A USB stick was then prepared with the bootstrap rendezvous information, and subsequently, one physical NSG was deactivated from the tenant which resulted in the associated physical NSG performing a factory reset on itself to remove all configuration data. We powered-off the NSG under test, inserted the USB stick into the USB port, and powered-on the NSG again. Simultaneously we generated Layer 3 traffic between the NSGs and observed 100% traffic loss. After 483 seconds, the NSG completed the bootstrap procedure and started the traffic flow without dropping any packets or requiring any configuration intervention. Please note, the 483 seconds include the "power-up" time of the NSG itself in addition to the bootstrapping process.

Conclusion

EANTC validated the scalability, functional capabilities, reliability and manageability of the Nuage Networks SD-WAN 2.0 solution extensively.

Based on the test results, we confirm that the Nuage Networks SD-WAN 2.0 solution meets Nuage Networks's claims, which are in line with the EANTC test requirements.

In our tests, the Nuage Networks solution scaled up to 4,000 NSGs and 396,000 bidirectional VxLAN tunnels servicing 40 tenants. In this scenario, the 4,000 NSGs were controlled by 20 VSCs. When configured with a single tenant, the solution successfully established up to 129,240 bidirectional VxLAN tunnels. No signs of throughput performance degradation were observed during this test.

In the multi-tenancy management area, the Nuage Networks SD-WAN 2.0 solution successfully demonstrated that it can attach a new tenant to the multi-tenant NSG and connect a new branch NSG with the newly added tenant without influencing existing tenants. At the same time, a multi-tenant NSG showed the ability to handle 40 tenants simultaneously in our tests.

The Nuage Networks SD-WAN 2.0 solution has the capabilities to add a new network service function chaining with the existing NSG without impacting the current running service. It supports adding a new customer site NSG with the existing tenant with minimal user interaction.

We also verified that the Nuage Networks SD-WAN 2.0 solution is equipped with a failover mechanism to help service providers maintaining operations during link and NSG failures.

The test results show that the performance monitoring tools function correctly within expected precision grades and that they can be used to provide visibility into application performance.

EANTC concludes that the Nuage Networks SD-WAN 2.0 solution supports large-scale tenant and branch site deployments well, including multi-tenancy management, resiliency, service chaining, and zero-touch provisioning.

About EANTC

EANTC (European Advanced Networking Test Center) is internationally recognized as one of the world's leading independent test centers for telecommunication technologies.

Based in Berlin, the company offers vendor-neutral consultancy and realistic, reproducible high-quality testing services since 1991. Customers include leading network equipment manufacturers, tier 1 service providers, large enterprises and governments worldwide. EANTC's Proof of Concept, acceptance tests and network audits cover established and next-generation fixed and mobile network technologies.

EANTC AG
Salzufer 14, 10587 Berlin, Germany
info@eantc.com, http://www.eantc.com/
[v1.0 20180926]