SCTE·ISBE CABLE-TEC EXPO 2019 NEW ORLEANS, LA SEPT. 30-OCT. 3

2019 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS

SD-WAN 2.0

A Platform For Multi-Cloud, Security And Value Added Services

A Technical Paper prepared for SCTE•ISBE by

Charuhas Ghatge
Senior Product and Solutions Marketing Manager
Nuage Networks, a Nokia Company
755 Ravendale Drive, Mountain View, CA94043
(510) 299-2989
Charuhas.ghatge@nokia.com

Table of Contents

List of Figures

Introduction

Enterprises worldwide have embraced the concept of SD-WAN, with leading telecommunications research firm IDC forecasting the worldwide market for SD-WAN to grow at a compound annual growth rate (CAGR) of 40% from $830 million in 2017 to more than $4.5 billion in 2022. Clearly, SD-WAN is here to stay.

SD-WAN 1.0 solutions have tried to solve the connectivity and automation challenges of branch offices, which have been underserved by the IP-VPN services. SD-WAN 1.0 also has been successful in reducing the bandwidth costs by offloading non-mission critical applications from the expensive MPLS to the cost-effective internet.

The new challenges for the enterprises are stemming from their quest and pursuit of Digital Transformation. The digital transformation almost mandates them to a multi-cloud strategy- from on-premises data centers to IaaS and SaaS public clouds and out directly to the branch offices and remote locations that constitute the intelligent edge.

With SD-WAN 2.0's reach from the branches to the DCs to the public clouds, security and governance become even more important as the attack surface increases, and hence the need for an end-to-end security model that is enterprise-wide: across hybrid-cloud, datacenter and branch network.

SD-WAN collapsed the functionality of a typical branch network, where many separate physical devices were needed to provide NAT, firewall, load balancers etc. into just one physical platform and many of these functionalities provided as VNFs. With the availability of this generic and powerful platform, the SD-WAN 2.0 must evolve this physical platform to deploy and manage Value Added Services including VoIP, Next Generation Firewall IoT and Wi-Fi access.

SD-WAN 2.0

1. The Challenges

Enterprise IT needs are unmet in providing Multi-cloud solutions, end-to-end-security and Transforming a branch to value added Services platform. Let us look at these unmet needs and challenges.

1.1. Multi-Cloud Solution

Hybrid Cloud has become the most popular approach to multi-cloud architectures. In Hybrid cloud you get the best of both worlds – the control and security of the private clouds and the flexibility and elasticity of the public clouds. Shortcomings in a wide area network (WAN) can exacerbate the complexity and management issue often associated with it. The network managers are often asking questions such as 'How can I easily move my workloads between public cloud providers and my branch or data center?' or 'How can I have fully redundant resilient connectivity using MPLS, Internet and LTE?'

1.2. End-to-End Security

Increasingly, the threat landscape is getting more sophisticated with the rise of ransomware, web-based malware, botnets and phishing emails resulting in significant financial loss and data breaches. Malware like WannaCry ransomware that used lateral movement shows the importance of ensuring proper

segmentation both at the branch and datacenter to contain lateral spread and the need for a new analytics-based approach to detect and respond to these zero-day attacks.

Massive data breach at Equifax is a reminder to organizations on the importance of patching and quickly closing security vulnerabilities to secure key data before an attacker can use the security gaps to steal personal information. Organizations continue to get breached despite investments in security. Clearly there are gaps in organization's current security model for these attacks to happen.

Current manual, perimeter-centric and reactive security model cannot effectively secure an organization data from emerging security threats in the cloud era.

1.3. Transforming the branch to a Value Added Services (VAS) Platform

The branch network of today is quite complex is comprises of many disparate physical devices offering spectrum of functionality and they include – NAT, DHCP, SBC/VoIP, security devices such as IPS/IDS, Firewall. They often are fragmented devices/appliances with rigid orchestration, they lack the flexibility to manage, configure and monitor and cost-prohibitive from the operational point of view. What is critically needed is a universal platform to ease the burden of manageability and flexibility to offer differentiated services at fraction of time and cost.

2. The Solution – SD-WAN 2.0

2.1. Multi-Cloud Solution

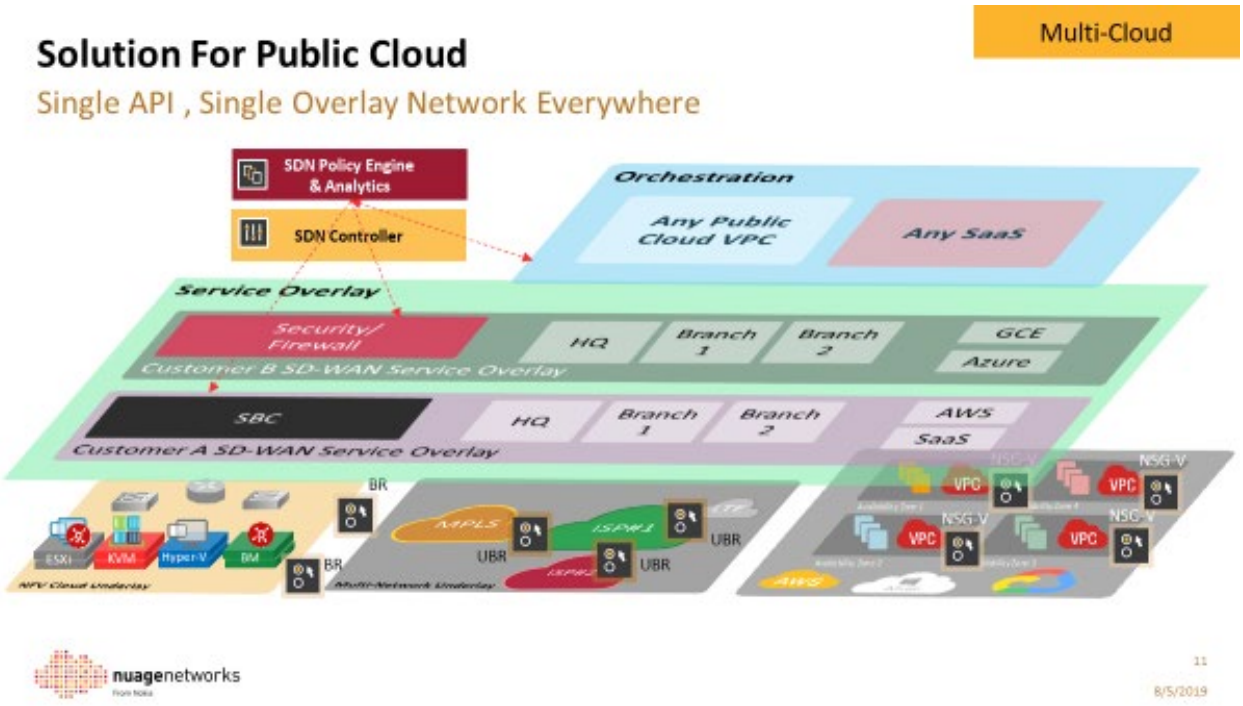

Figure 1 - Solution For Public Cloud

SD-WAN with its overlay feature, must provide the flexibility and choice of multiple underlay networks, whether those networks are MPLS or internet (from multiple ISPs). An ideal SD-WAN multi-cloud architecture should provide:

- Underlay
  - NFV DC underlay (private cloud underlay)
  - Multi-network underlay (MPLS, Internet- from multiple ISPs and LTE)
  - Public Cloud (AWS, Azure, GCP) Underlay
- A SD-WAN Services Overlay
  - Orchestration, Analytics and Policy Engine.

2.2. End-to-End Security

While microsegmentation provides significant benefits in terms of reducing the attack surface by limiting lateral movement of malware inside datacenter and cloud, organizations need a comprehensive security model that is enterprise-wide: across hybrid cloud, datacenter and branch network.

Gartner defined a new security approach called Adaptive Security Architecture, one that is beyond traditional prevention and detection **and includes response based on continuous monitoring and analytics**. This adaptive security model suggests organizations to move from "incident response" mindset to a "continuous response" to defend against new wave of security threats.

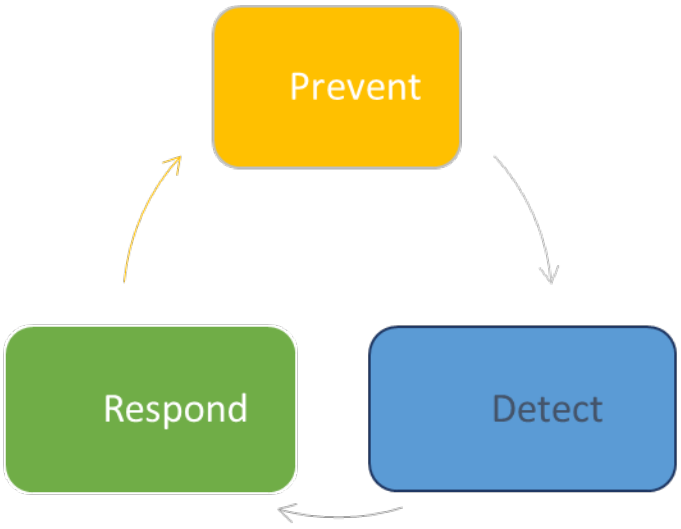

Figure 2 - Adaptive Security Model

2.2.1. *Prevent*

This phase of the security implementation, as the name suggests, prevents various attacks at various points and layers in the network.

2.2.1.1. L3-L4 Stateful Distributed Firewall

- Limit branch user access to/from internet as well as data center using L3-L4 stateful security
- Validated by 3rd party auditors for PCI-DSS 3.2 network firewall requirements

The Payment Card Industry (PCI) Data Security Standard (DSS) is one of the most wide-reaching standards since virtually every enterprise has individuals or organizations conducting transactions that accept, process or receive payments. Whether safeguarding payment information is an integral part of the core business – as in online retail and financial services – or an important aspect of the core business

(such as internal purchasing departments, consumer payments for services provided in the public and private sector), compliance with PCI DSS standards is essential.

- Logging of ACL actions for compliance and auditing

Logs of ACLs that are configured on the firewall can provide valuable information for auditing and subsequently for compliance. The ACL logs provide information about the packets that match an ACL such as source/destination IP, source/destination port and the protocol (TCP/UDP). The logging of ACL actions provides crucial information for auditing as well.

2.2.1.2. Layer 7 Application Control

- Restrict branch user access to specific applications using L7 DPI

With the ability to do Deep Packet Inspection (DPI) and to recognize 100s of application signatures, the administrator can define security policies that restrict or allow any of the recognized applications for any user.

2.2.1.3. SaaS Application Control

The SaaS services have become very prevalent in the enterprise IT environments. These SaaS service definitions should be recognized by the SD-WAN security engine such as Office365, WebEx, Salesforce, GitHub, JIRA, Azure, AWS and Google. These pre-defined SaaS services can be used in application identification, definition and ACL control.

2.2.1.4. Web/URL Filtering

- Blocks branch user/device access to malware as well as inappropriate content
- DNS based enforcement based on filtering DNS queries to internet sites

An internet site can be blocked or allowed, based on the DNS lookup. If an internet site is to be blocked, DNS query for that site is not returned to the requester. If it is allowed, then an IP address is returned to the requester.

- Supports content/website category based filtering (e.g., block malware, block adult content, block streaming media)

Websites categories are assigned to websites based on their dominant Web content. A website or webpage is categorized into a specific category that is likely to be blocked according to its content. When a website contains elements in different categories, web pages on the site are separately categorized. The categories are defined to be easily manageable and patterned to industry standards. There are many such categories and examples include adult content, dating sites, gambling or even can be categorized based on bandwidth consumption such Internet Radio and TV, Streaming sites, peer-to-peer file sharing etc. SD-WAN Security engine should support many of such website categories with over 32 billion URLs/domains that have been categorized.

- Supports filtering based on custom blacklist/whitelist of websites including wildcard matches

Custom blacklists and whitelists can be created and defined. Filtering of the traffic based on these blacklists and whitelists is supported.

- Supports logging of blocked websites/categories

Any blocked website or category is logged if trying to access that site/category.

2.2.2. *Detect*

Continuous detection needs to be an ongoing part of security within a cloud-based environment. Typically, the new breed of attacks is more nuanced and sophisticated, unlike a typical Denial of Service (DOS) attack. These attacks could be zero-day attacks with no known signature and designed to permeate and infect laterally (east to west). Using flow analytics, traffic flows for each application need to be tracked throughout the application's lifecycle to anticipate potential threats.

2.2.2.1. Contextual Flow Visualization

The right solution should also leverage traffic insights from existing installed security measures. By correlating analytics from installed security measures with existing flow analytics (Flow Explorer), further contextual insight into the traffic and potential threats will be unlocked. For example, has this traffic attempted to breach any of the security controls that have been established and if so to what degree? Having access to this information will provide more context and will allow the enterprise to intelligently automate remediation policies.

2.2.2.2. Top Talkers

Top Talkers gives you topN source and destination pairs that are most talkative. A very handy functionality for identifying who is consuming most bandwidth and potentially attempted attacks.

2.2.2.3. L3-L7 Traffic Visibility

By setting thresholds and alerts based on those thresholds, allows one to proactively monitor and alerts and alarms if certain thresholds are crossed (rising as well as falling).

2.2.3. *Respond*

Automated Policy Action

By having a dynamic understanding of the application traffic within the perimeter of the data center, branch, or public cloud, enterprises can then define and implement automated policies that can respond to certain suspicious application traffic flows in real-time. Some examples include:

- Real-time local alerts can be triggered informing the operator of suspicious activity for each application right down to the service-tier level of granularity. For example, an alert can be triggered when a certain TCP port on a virtual DB server is receiving an unexpected amount of ingress traffic
- Suspicious traffic can be steered to an existing SIEM to provide more correlation and analysis on this suspicious traffic flow, or to an IPS or L7 FW to sanitize the traffic
- Suspicious traffic can be quarantined or even blocked by steering traffic into a quarantined zone based on an automated trigger.

2.3. Transforming a branch to a Value Added Services platform

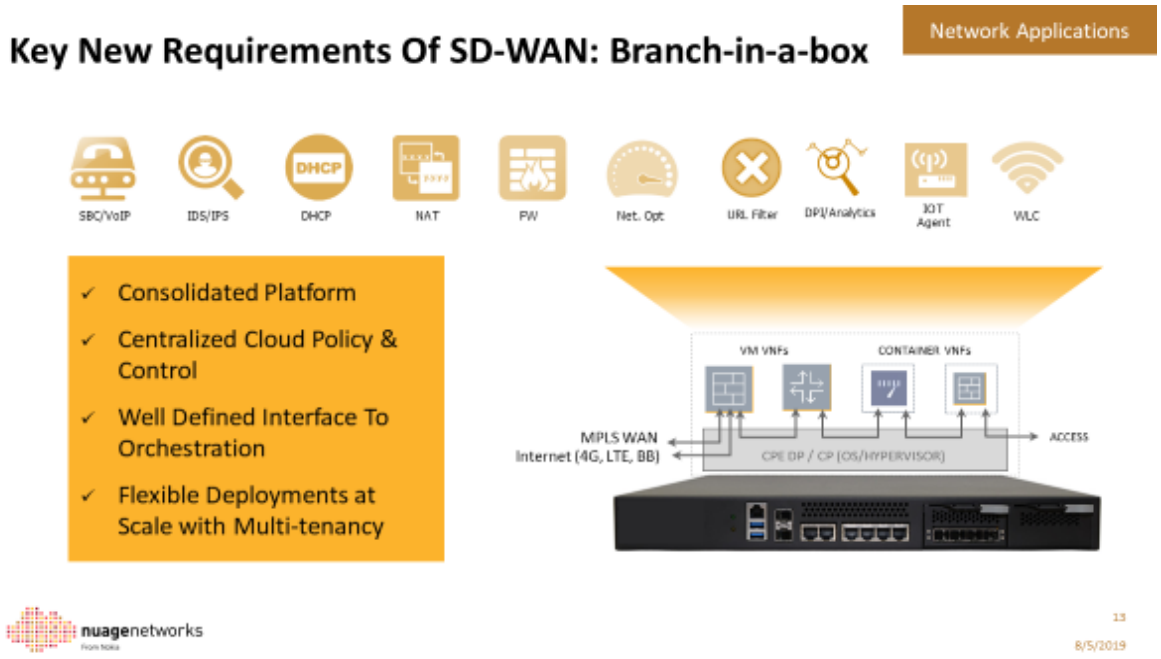

Figure 3 - Key New Requirements of SD-WAN: Branch-in-a-box

Conclusion

SD-WAN has been a technology in the recent past that has succeeded and lived up to its hype because of the cost benefits, implementation flexibility and amalgamation of pragmatic technologies. However, with the advent of digital transformation and the relevant cloud transformation and security requirements, SD-WAN 2.0 is an evolution in offering multi-cloud integations, pervasive security and transforming a branch as a Value Added Services (VAS) platform.

Abbreviations

ACL	access control list
DNS	Domain Name System
DOS	denial of service
DPI	deep packet inspection
IoT	Internet of Things
IPS	Intrusion Projection System
LTE	Long Term Evolution
MPLS	Multiprotocol Label Switching
SaaS	software as a service
SDN	Software Defined Network
SD-WAN	Software Defined Wide Area Network
SIEM	Security Information and Event Management
URL	uniform resource locator
VoIP	Voice Over IP