VIRTUAL EXPERIENCE
OCTOBER 11-14

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

SD-WAN Security and SASE

How to Secure SD-WAN and Role Of SASE

A Technical Paper prepared for SCTE by

Charuhas Ghatge
Senior Manager, Product and Portfolio Marketing
Nuage Networks by Nokia
520 Almanor Ave, Sunnyvale CA
(510) 299-2989
Charuhas.ghatge@nokia.com

Table of Contents

List of Figures

List of Tables

1. Introduction

Software-defined wide area networks (SD-WAN), a software approach managing wide-area networks, offer ease of deployment, central manageability, and reduced costs, and can improve connectivity to branch offices and cloud. End users are excited about SD-WAN because it enables them to manage and add network functionality using a cloud-first strategy for application access and delivery.

Compute resources and associated cloud services are exploding, and traditional enterprise network boundaries have expanded into the public cloud, branch locations, and intelligent edges. So, what does this all mean to the branch security?

Cloud computing has created several challenges since networking and security are incompatible with the cloud-centric and mobile-first business models. The network is rigid and static. Security is heavily centered around the data center, fragmented across multiple domains of physical locations, cloud resources, and mobile users. Networking and security have created silos that were built and implemented decades ago, and new functionalities are added and patched in as needed in a haphazard way. Secure Access Service Edge (SASE) is a new paradigm defined by Gartner that combines network and security into a single cloud-based service.

In this whitepaper, we will discuss SD-WAN security features and explain SASE – what is SASE, why is it needed, what does it comprise of and its deployment considerations.

2. SD-WAN Security

Existing security models cannot effectively address the new security requirements driven by move to cloud and the evolving threat landscape.

First, due to SD-WAN allowing the use of broadband internet as a transport mechanism, the internet, which is traditionally not a guaranteed secured link, the access to it needs to be made secure.

Second, current protection model in Enterprise branch is basic and not enough to secure local internet breakout to cloud as all traffic is steered over Multiprotocol Label Switching (MPLS) to Data Center (DC) sites where security is applied. Also, there is not much end to end micro-segmentation between branch and DC/cloud applications across the enterprise.

Third, with the increasing attack sophistication and evolving threat landscape we cannot assume that all attacks can be prevented by protective controls. Currently there is not much visibility to branch user traffic. Visibility and security analytics are key to help detect attacks.

Last, but not least, the current security provisioning model for applications is largely manual and device-centric.

Major security functions for a secure SD-WAN are discussed in the subsections below.

2.1. Securing broadband internet access

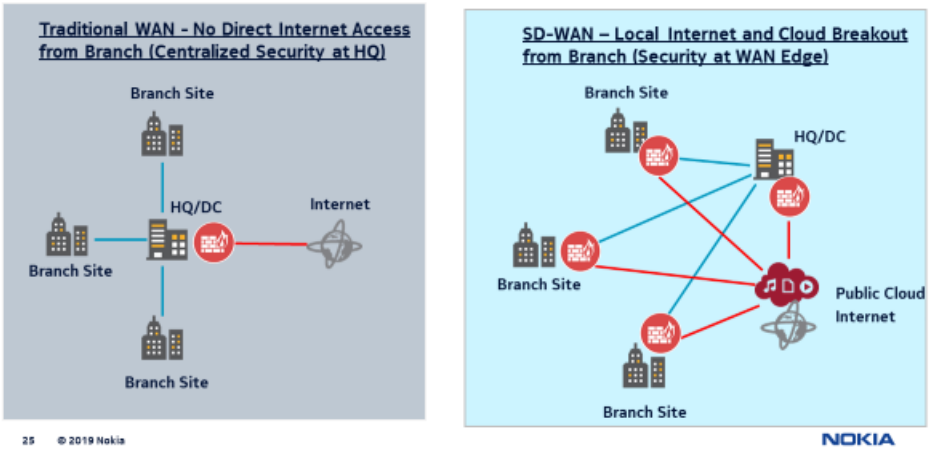

Figure 1 - Local Internet breakout

The Internet is not very secure for enterprise WAN requirements. Hence cloud-based application traffic is often backhauled from the branch to the enterprise Headquarters (HQ) before being handed off to the Internet. This introduces delay and jitter and hence application performance is often compromised because of WAN bandwidth constraints at the branch and added latency from backhauling connections.

The solution is to use direct internet connectivity to the cloud and web applications from the branch. The SD-WAN solution needs to make these internet connections secure and reliable by creating encrypted tunnels between every site in the SD-WAN, while taking advantage of Secure Socket Layer (SSL) security provided by the Software as a Service (SaaS) application for traffic going from the branch to the application directly using the Internet. This makes the Internet access more secure. With such encrypted links and a stateful firewall, an SD-WAN solution can prevent unauthorized outside traffic from entering the branch. The stateful firewall is usually implemented directly on the Customer Premise Equipment (CPE) device of the SD-WAN and no external security hardware or software should be needed for the stateful firewall functionality.

2.2. Threat prevention using IDS and IPS

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are important to detect and prevent the known attacks by recognizing the virus signatures. Threat prevention component prevents malware from penetrating the network, regardless of application traffic in which they are hiding. It is important that the IDS/IPS functionality should be implemented natively on the CPE of the SD-WAN.

It uses signatures of known attacks to match traffic that passes through the CPE to prevent attacks and these signatures have been divided into groups of relevant signatures. IPS/IDS policies can be defined and managed centrally via the SD-WAN GUI or APIs. It is recommended that signatures be updated dynamically from cloud and applied on the local CPE device of the SD-WAN. The SD-WAN GUI should display statistics and generate reports of intrusion event details rule hit counts etc.

2.3. Stateful Firewall

A stateful Firewall filters packets based on the state and context of network connections and provides full protocol inspection considering the STATE+ CONTEXT of the flow, thereby eliminating additional attacks surface.

A stateful firewall understands the network flow and can identify data packets of a flow. Since a stateful firewall can look deeper into packet payloads, it can support DDoS (TCP/UDP/ICMP Flood), Port-scans etc.

Step one is to secure the branch within the SD-WAN network and to secure the links for the internet breakout. This is done by implementing a stateful firewall right on the CPE device without any additional external equipment or implementing any third-party solution. This way local branch users can safely access the corporate resources and SaaS applications in the cloud while being protected from both, inside and outside threats.

Enterprises can define access rules and policies to allow or deny traffic to/from the application – for example the administrator can define a policy to deny access to cloud storage app that is not in the corporate IT's management domain. There could be a policy allowing access to an application like say, Office365.

Note that, Stateful Firewall should preferably be validated by 3rd party for PCI-DSS network firewall requirements.

2.4. Threat Intelligenece based on IP Reputation

Threat Intelligence feature detects branch device communication to risky IP addresses and sites. It also generates reports on access to risky IP and sites from SD-WAN branch user devices. Threat Intelligence uses IP reputation database that is updated daily from cloud.

2.5. Web/URL Filtering

URL filtering limits access by comparing web traffic against a database to prevent employees from accessing harmful sites such as phishing pages. Users spend increasing time on the web, surfing their favorite sites, clicking on email links, or utilizing a variety of web-based SaaS applications for both personal and business use. While incredibly useful to drive business productivity, this kind of unfettered web activity exposes organizations to a range of security and business risks, such as propagation of threats, possible data loss, and potential lack of compliance.

2.6. L7 and SaaS Application Control

One of the prime benefits of SD-WAN is its ability to allow a direct access for a branch user to the cloud and SaaS applications. A good secure SD-WAN must have the ability to restrict user access to a specific

application, be able to set application-based policies and monitor and log application usage. For this, it needs to have a layer-7 Deep Packet Inspection (DPI) engine to recognize thousands of application types and pre-defined SaaS services - Office365, WebEx, Salesforce, GitHub, JIRA, Azure, AWS, Google among others for easy access as well as monitoring.

2.7. Automated and rapid response to threats

A rapid and efficient incident response continues to be the biggest challenge facing security teams today. The sheer volume of these signals means that a lot of critical alerts miss getting the timely attention. Security teams need help to scale better, be more efficient, focus on the right issues, and deal with incidents in a timely manner.

By defining automated response action, the users can prevent malware from infected branch device from entering corporate network. For example, leverage network security analytics to identify suspect end-points based on threshold alerts and use service chaining to dynamically insert services (such as NGFW or IPS) for suspect traffic. The suspect traffic could be diverted to cloud-hosted security service.

2.8. Realtime security analytics and automation

Some threats can be quite sophisticated and cannot be prevented by the protective methods. Real time traffic monitoring and security analytics provide fine granular visibility to locate the cause and reprogram the security response. Automated action reduces the time to react to the anomalies and reduce the impact.

With end to end visibility and control for each application, the operator can detect, protect resources at a very granular level, and use automation to respond in real-time to threats. SD-WAN security monitoring should allow you to do a contextual flow visibility of each flow.

Realtime security analytics helps in Threat hunting, Network Forensics as well as troubleshooting. The forensic reports can be used for compliance and security audits – both internal audits as well as external agency audits.

Realtime network security monitoring allows you to generate alerts based on security events - port scan detection, port sweep detection, security policy violations and volumetric DDoS attacks.

3. Third-party Security Technology Ecosystem

Third-party security products should be a part of the overall effective security functionality for an SD-WAN solution. Third-party security solutions should be incorporated in a couple of ways:

Most enterprises have an existing set of security infrastructure and solutions they use. SD-WAN vendor should partner with the best of breed security appliances already present in the IT infrastructure.

Secondly, for a tighter alignment with the security vendors' advanced functionality, the security VNFs (Virtual Network Functions) from those vendors should be integrated onboard the CPE. Both these options are described below.

3.1. Security partners and Cloud Security services

When it comes to security, it's simply not feasible for a single SD-WAN vendor to provide every security functionality on its own. The scope of threats, risks, and corresponding technologies is simply too great. SD-WAN vendor should establish technology partnerships covering several security domains, such as industry-leading next-generation firewalls and secure web gateway and Cloud Security services.

The integration with a Cloud Security vendor allows you to route local branch Internet-destined traffic directly to the security cloud to enable a fast and secure experience This eliminates the need to backhaul local traffic to the internet gateway.

You can route specific traffic to the Cloud Security vendor's security cloud through IPSec tunnels for further security. For example, you can define an action to route the traffic to Cloud Security vendor's cloud as part of the response to a threat.

3.2. Hosted VNF on CPE and Service Chaining

The CPE of the SD-WAN solution also acts as a powerful platform to host VNFs. SD-WAN implantation should have the service chaining functionality. By service chaining the VNFs (many a times, on-demand), a dynamic and advanced security features are provided.

4. Secured Access Service Edge (SASE)

4.1. Overview – What problem is being solved by SASE

As cloud becomes pervasive and driven by digital transformation of enterprises, the networking and security needs of an enterprise are evolving. Traditional enterprise network and security paradigm was centered around applications in private data centers. Although networking was complex, the security risk profile was well defined. Migration of applications to the cloud has redefined the networking and security. Many companies use SD-WAN to securely connect branch offices to their corporate networks instead of relying on traditional and expensive MPLS links. SD-WAN also facilitates direct access by corporate branch offices to the public clouds and SaaS applications. This creates stringent security requirements from the branch to the cloud.

Gartner observed this trend of security and networking requirements and has recently defined a new framework that converges network (SD-WAN) and security into a single cloud-based service: Secure Access Service Edge (SASE).

This section discusses what is SASE, it's advantages, key components, deployment options and recommendations for a successful SASE implementation.

4.2. What is SASE and its key components

SASE is a framework that brings together networking and security services in one unified solution designed to deliver strong security from edge to edge, delivered as a service. It is not an RFC or a static architecture, but rather a recommendation and a framework.

SASE has two major functional blocks – Networking (SD-WAN) and Security, as shown in figure x. SD-WAN is the foundation of SASE and security features are offered on and beyond SD-WAN.

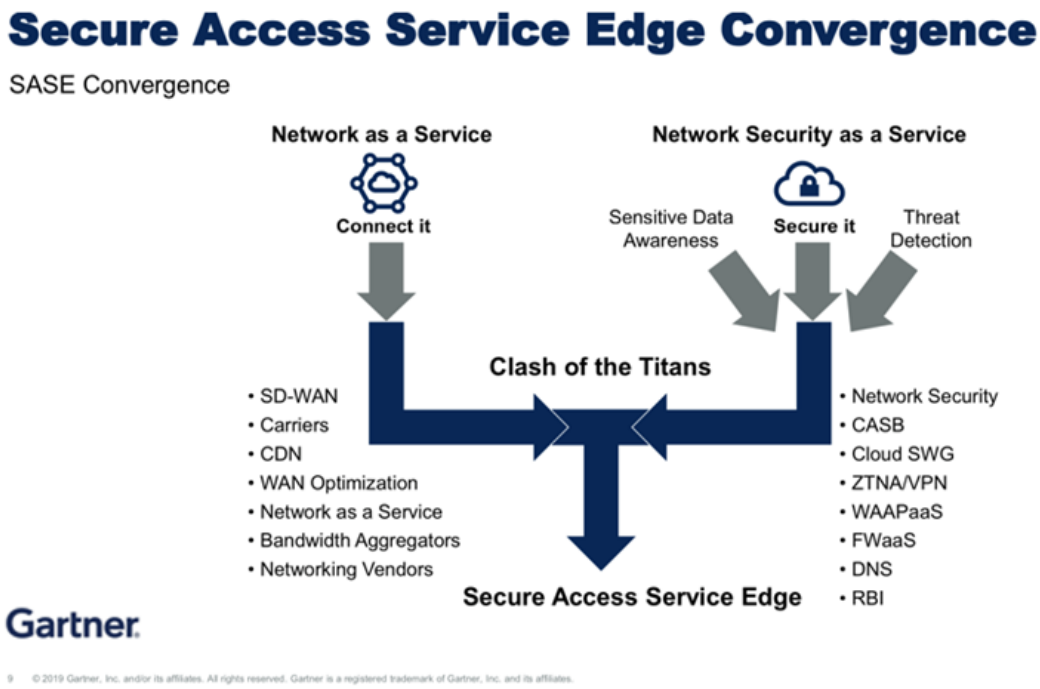

Figure 2 - SASE Components

4.3. SASE Networking (SD-WAN) – features and benefits

SASE networking capabilities offers the following benefits and capabilities:

- Network Agility – Flexibility and choice of MPLS, broadband or LTE.
- Multi-Cloud and SaaS Connectivity without the need for backhauling.
- Network Management and Automation - Real-time network monitoring, analytics, and reports.
- Application Performance Assurance – Business-policy based application prioritization.

Table 1 - SD-WAN Features and descriptions

Feature	Description
Comprehensive Routing capabilities	Full stack of routing protocols to support switching and routing personalities
Access and Connectivity to and from Anywhere	Seamless connectivity and policy management across fixed (internet, L2 and L3) and mobile WANs
Performance based POP selection	Support for multiple paths and POPs and performance-based selection ability
Application aware routing and traffic steering	Providing optimal application experience based on application types

Feature	Description
Hybrid WAN support (Full MPLS/Ethernet) for legacy Datacenter access	Seamless integration of existing networking to access data center and apps
Multi-Cloud & Hybrid Cloud connectivity	Policy based access to and across applications in private cloud and multiple public clouds
Connectivity Security – VPN, IPSec	Embedded encryption and end point security
SD-WAN Service Portal	Multi-tenant SD-WAN portal hosted by CSP for the visibility and control the CSP service and operations teams need to manage multiple SD-WAN services.
WAN Optimization & Bandwidth Aggregation	Optimizing the use of available network for availability and performance

4.4. SASE security components

Table 2 - SASE Components

Component	Description
IPS	Intrusion Prevention system
IDS	Intrusion Detection System
Firewall	Stateful Firewall
Realtime Security Analytics and Automation	With end-to-end visibility and control for each application, the operator can detect, protect resources at a very granular level, and use automation to respond in real-time to threats.
SWG and DNS Filtering	Secure Web Gateway is used to protect users and devices from online security threats by enforcing internet security and compliance policies and filtering out malicious internet traffic
ZTNA	Zero Trust Network Access
CASB	Cloud Access Security Broker - According to Gartner, a cloud access security broker (CASB) is an on-premises or cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed.
DLP	Data Loss Prevention - DLP provides visibility across all sensitive information, everywhere and always, enabling strong protective actions to safeguard data from threats and violations of corporate policies.
FWaaS	Firewall as a Service

4.5. Deployment considerations for SASE

SD-WAN, although a new technology, has been maturing in recent times and the number of deployments is growing rapidly. The security technology including cloud-delivered security is mature and most enterprises have deployed security in some form or other. Given this, a SASE deployment of rip-and-replace is not practical because of the existing investments. The most pragmatic solution will consist of utilizing existing security, especially cloud-delivered security to offer SASE. SD-WAN's flexibility to integrate with existing security vendors is very important. A complete SASE solution from a single vendor would compromise completeness due to vendor's technology limitations, it will reduce flexibility in a very dynamic space of enterprise security, and it will also risk the vendor lock-in. It should also be noted that MEF has specified SD-WAN standards, however, the security architecture is and likely will continuously evolve.

So, a good SASE solution should have the flexibility of:

- Scalable, high performance SD-WAN because SD-WAN forms the foundation of SASE.
- Exhaustive natively embedded security functions within SD-WAN itself.
- Integration with cloud security vendors for advanced security functions, as well as, evolving capabilities in this space.
- Ability to deliver SD-WAN as well as security features via Managed Service Provider or MSP partners' cloud and POPs.

This flexibility will allow the Managed Service Provider to offer cost effective SASE solutions based on its enterprise customer's specific needs rather than one size fits all expensive approach. It will enable MSP to differentiate its offer from other cookie-cutter (me too) solutions.

5. Conclusion

Since, SASE is a framework, rather than a standard, each vendor's implementation is unique to that vendor, depending on their expertise. Also noteworthy is that, like any new technology, there is a hype cycle and then there is reality. Currently, SASE is at the peak of its hype cycle. We believe, and Gartner agrees, that SASE is a 5-10-year journey versus a defined destination.

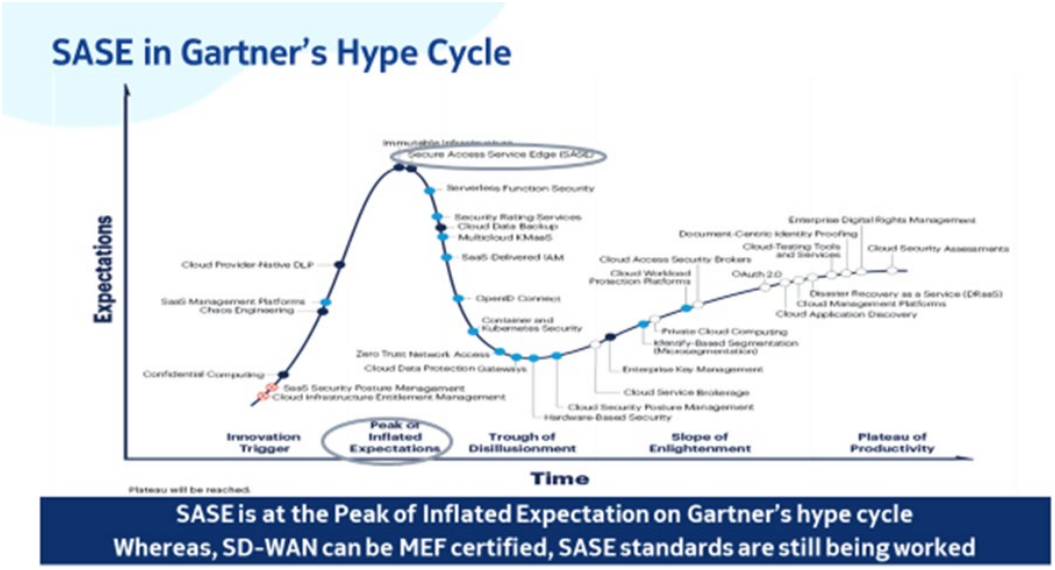

Figure 3 - Gartner Hype Cycle

Considering this, an MSP should opt for a solution that provides strong foundational capabilities and at the same time provides flexibility to evolve the solution in a vendor agnostic manner.

SD-WAN is being widely adopted by enterprises, greatly simplifying the branch network environment by integrating multiple functions (Internet and hybrid WAN connectivity, Advanced Security & NGFW, Cloud on-ramp, Application Experience, Wi-Fi, etc.). The SASE platform provides another strategic advantage for MSPs to offer SASE, a comprehensive networking and security solution, as a Service. With its foundational SD-WAN capabilities, advanced security embedded within the platform, and open vendor-agnostic platform affords MSP a future-proof SASE solution.

Abbreviations

AWS	Amazon Web Service
CASB	Cloud Access Security Broker
CDN	Content Delivery Network
CPE	Customer Premise Equipment
CSP	Communications Service Provider
DC	Data Centre
DLP	Data Loss Prevention
DNS	Domain Name System
E2E	End to End
FWaaS	Firewall as a Service
GCP	Google Cloud Platform
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSec	Internet Protocol Secure
MEF	Metro Ethernet Forum – An Industry consortium defining SD-WAN standard
MPLS	Multi-Protocol Label Switching
POP	Point of Presence
SASE	Secure Access Service Edge
SD-WAN	Software Defined Wide Area Networking
SWG	Secure Web Gateway
WAAPaaS	Web Application and API Protection as a Service
WAN	Wide Area Network
ZTNA/VPN	Zero Trust Network Access / Virtual Private Network

Bibliography & References

Secured Access Service Edge (SASE) – Gartner, 2019

