SD-WAN Explained - What is Software Defined WAN (SDWAN)

Software Defined Wide Area Network (SD-WAN) is a centrally managed network that allows enterprises to utilize different, and typically lower cost, WAN interfaces such as broadband and wireless networks for creating their enterprise network architecture in an agile and customizable manner. This article will delve into the details of what is an SD-WAN solution, SD-WAN benefits, and the promise it brings to enterprise WANs. Although SD-WAN products and SD-WAN services differ in their characteristics, this article will review the common concepts introduced by SD-WAN vendors and what SD-WAN vendors strive to achieve by following the traditional business concepts of large networking vendors. Finally, we will also refer to the introduction of open-source SD-WAN and the technology and business changes it brings to this market. But, before getting into all these topics, let us first look at the history of WANs and how enterprise WAN requirements help define what is an SD-WAN solution of today and how it applies to future enterprise network requirements.

The History of Wide Area Networks (WANs)

Wide Area Networks (WANs) connect users and devices across many locations to services, applications, and data that reside in data centres and cloud providers. Every 10 – 15 years, WANs go through a revolution on how they are designed and built. Early WANs used modems to transmit data over phone networks.

Second generations used frame relay and ATM, and third generation WANs used MPLS. Software Defined Wide Area Networks (SD-WANs) are the fourth and most current generation of WANs. Traditional WANs are designed to serve traditional network architectures and requirements of businesses. In these architectures, the focus was on applications served from self-owned or private data centres thus, utilized dedicated lines that were typically MPLS. Enterprise networks designed to support these requirements are not relevant for current and future enterprise needs. As applications move to the cloud, a growing need for network agility, application variety and increasing user mobility, networks need to evolve, welcome to SD WAN.

SD-WAN Architecture

The definition of what is an SD-WAN solution and the architecture of SD-WAN varies between SD-WAN vendors and SD-WAN service providers. In high level, SD-WAN architecture comprises a central management system (typically hosted in the cloud) and many edge devices that are basically routers with additional capabilities. Since common SD-WAN benefits revolve around secured connections between enterprise locations and their connectivity to cloud services using non-dedicated (e.g. broadband & LTE) connections, these edge devices should come in the form of SW instances that can be installed in the cloud, on virtual machines or on general purpose hardware devices. Below are a few common attributes that would help define what is as SD-WAN solutions:

- Overlay & underlay – Separating the network layer from the applications
- Separation of data & control
- Tunnels between sites and the cloud
- Policies – application, quality of experience, security

- Local internet breakout – Direct Internet Access (DIA) is typically possible depending on the architecture of the specific solution and its deployment

SD-WAN Benefits

SD-WAN vendors build their solutions in different architectures and philosophies. If you would ask a network administrator that deployed SD-WAN what is an SD-WAN and what did his/her organization gain from it, the typical answer would include the following SD-WAN benefits:

- Faster
- Better
- Lower cost
- More secure

Faster

Faster networks – The disaggregation of transport and applications where enterprise networks become transport agnostic, allow to utilize multiple WAN interfaces for achieving better (faster) application delivery to end users. SD-WAN services typically offer the capabilities for defining routing policies based on business needs (application prioritization and quality of experience-based decisions), this is one of the primary pillars of what is SD-WAN technology. Typically, SD-WAN vendors offer in their products or services the option to route traffic from branch offices directly to the internet. This option of Direct Internet Access (DIA) is an important requirement for improving the speed of your network. Some of the SASE services do require backhauling all traffic through central points of presence and over a dedicated backbone of the SASE service provider. This network architecture should be carefully examined as in many cases, it increases

latency and results in higher cost. Although Gartner does include backhauling of data through cloud POPs in its recommendation, one needs to consider this recommendation with reference to its specific enterprise requirements for performance, security, and cost.

Agile network architectures – Network agility is also an important item on the SD-WAN benefits list. Different from traditional WANs, being software defined and centrally managed, network architecture of hub and spoke, full mesh or any combination of these architectures, can be quickly provisioned and changed as required on SD-WAN networks. Different from the fixed nature of traditional networks, SD-WAN architecture gives agility in the hands of network administrators, through automation, network performance may grow and shrink as workloads and associated business requirements change. Backup network interfaces may be added or removed as network requirements change. This completely changes the traditional paradigm of fixed connectivity contracts and network designs that inhibited flexibility.

Better

Reliability of the network – One of the important SD-WAN benefits relates to network reliability. In the past, a site would lose its connectivity due to failure of a single dedicated line that serves the site. Even if several connections were available, the routing policies would be fixed so some of the applications or users in the organization would lose their connectivity in the case of such network failure with no way for network admins to define dynamically policies based on importance of services or users. SD-WAN changes this as a typical SD-WAN product would allow to define failover and load balancing policies that would ensure better and more reliable delivery of specific applications even

when network conditions deteriorate or even in cases of specific network interfaces failure. This benefit of network reliability is one of the key elements of what is an SD-WAN solution all about. Network automation – Both on-boarding of new locations as well as the on-going operation of the network and adaptation to changing network conditions and workloads are automated in SD-WAN. Through zero touch provisioning (ZTP) devices are connected to power and ethernet and automatically provisioned in the central management system. Policies for changing routing logic are defined and pushed to network edge devices from this central management system and come to action automatically as changes are identified by the system. Additionally, DevOp tools can be utilized so that networking bandwidth and associated routing and security policies can be provisioned dynamically as compute and storage change.

Cheaper

Reduced OPEX (operational expenditure) – Being transport and service provider agnostic is another pillar of SD-WAN benefits. An enterprise can choose which Network Service Providers (NSP) to purchase connectivity from, moreover, the enterprise can purchase several types of network connections such as broadband, 4G or 5G cellular connections or even MPLS, define the utilization of these different network connections based on quality, cost, and other enterprise requirements. Additionally, such policies can be dynamically changed from one central management system. The nature of centrally managed SD-WANs also results in the reduction of IT people required for managing the network, instead of logging into each edge device and configuring it through a Command Line Interface (CLI), all edge devices can be centrally configured and managed.

Reduced CAPEX – This is one of those SD-WAN benefits that is many times neglected in the decision-making process. Although one of the promises associated with the definition of what is SD-WAN was hardware agnostic, some of the SD-WAN vendors continue to require a bundle of hardware and software resulting in high Total Cost of Ownership (TCO) and greater vendor lock-in. Being hardware agnostic is an important requirement enterprises and service provider should present to SD-WAN vendors. Being able to run on commodity hardware devices, on virtual machines or in public/private clouds gives enterprises choice, more control and lower capital costs.

More secure

End-to-end encryption – Most of the cloud SaaS (Software as a Service) applications encrypt the traffic of their applications, but not all enterprise data sent between locations is encrypted. Even many of the voice and video communications services do not encrypt the payload (the actual data of voice and video). The SD-WAN architecture typically allows for secure (encrypted) tunnels between locations of edge devices (software and hardware) thus making sure that all traffic in motion will be encrypted. In this regard, it is important to analyse the architecture of some of the SASE vendors. When looking at the Gartner definition of recommended SASE architecture, you would find a fixed network architecture of hub and spoke where all enterprise traffic is routed through cloud Points of Presence (POPs) of the SASE vendor or service provider. This SASE architecture would typically require a man in the middle decryption of the traffic. It does not mean that this type of SASE network architecture does not have merit, it does mean that enterprises should understand the details of how the SASE service is provided to them and understand the pros and

cons of each option. flexiWAN allows for more flexibility and choice in all relevant areas of SD-WAN and SASE deployments. This includes network architecture, routing policies, the security services used and how each specific data or application is routed according to those selected choices of security and network architectures.

Zero trust networks – This capacity of zero trust is one of the SASE benefits although it is not always offered by all SASE vendors. Given the strong relationship between SASE and SD-WAN, zero trust is also achieved with secure SD-WAN solutions. Providing 1:1 micro-segmentation between users and devices communicating with services, applications, and data. Whitelist security policies of what is allowed in a least privileged model instead of a blacklist model that defines where network traffic cannot go. Anomaly detection provides early detection if a user is misbehaving, or a device has been infected with malware.

SD-WAN standard

There is no standard protocol for SD-WAN but there are several attempts to standardize some areas of SD-WAN. Standards are required for things to work one with the other, the reason you need to carry electrical adapters when you travel from the US to Europe is because there is no one agreed world standard for how power outlets should look like. In communications, standards are created so product of company A will work with the product of company B. In practice this means that standards are required in 2 areas:

- APIs (Application Programmable Interface) – this is why you can browse this website from any standard browser
- On-the-wire protocols – this relates to the structure of the packet, the transport protocols used and encryption algorithms

Standardizing SD-WAN APIs and the on-the-wire protocol would allow enterprises and service providers to use multiple SD-WAN products in their network, interconnect between different SD-WAN vendors and manage all SD-WAN products in their network from one unified management system. This is a dream many service providers would like to realize, SD-WAN vendors are less keen on this. So far, the attempts to create a standard for SD-WAN have not been successful, this is mainly due to the following reasons:

- Large vendors are not always happy to participate in this initiative, while they usually lead and fund standard bodies, they do not always fully comply with the standards created. A good example for this is VoIP products, while the leading product vendors (some happen also to be leading networking vendors) lead many of the IETF standards, their products do not interwork with edge devices (phones) of other vendors thus create a strong vendor lock-in
- The protocol structure of SD-WAN products is typically specific (proprietary) based on the SD-WAN vendor. Although SD-WAN vendors use standard protocols in their products, they add proprietary elements to the protocol, add-on that increase reliability, allow for better network monitoring and other features
- Also, on the management and configuration side, SD-WAN products differ in what they offer avoiding the option to standardize the management layer
- Efforts for creating an SD-WAN standard have been placed on areas that are not necessarily required to be standardized, the SD-WAN product itself and the features of an SD-WAN service should be left for the industry, avoiding standards in the product level will allow for variety and innovation

SD-WAN Standard work so far has been conducted by the following bodies:

- MEF – work is focused on 2 areas:
    - MEF 70 defines an SD-WAN standard for SD-WAN services and its service attributes. This SD-WAN service standard is part of the MEF 3.0 service framework. This standard is geared towards SD-WAN service providers and enterprises contemplating on which

service to use. The challenge of defining a service (in general and to greater extent by an organization with many paying members) is the need to answer the requests of competing service providers typically resulting in a low common denominator of the requirements. Having said that, this work does help enterprises who are starting their SD-WAN study in the journey to define their needs but should not be the only resource used for this purpose
    - LSO – Life Cycle Orchestration – This work goes beyond SD-WAN as its goal is to standardize the management and control across all network domains responsible for delivering an end-to-end Connectivity Service (e.g., Carrier Ethernet, IP VPN, MPLS, etc.). An SD-WAN product can implement the relevant APIs to allow for unified management of multiple SD-WAN vendors. These APIs have not been widely adopted by SD-WAN companies to be included in their products
- IETF – The IETF is the standards body that practically defines the internet and networking protocols; hence, it is probably the right entity to take the lead on defining an SD-WAN protocol. The IETF has focused on defining YANG models for an SD-WAN service provider services orchestrator to provision, configure, and manage the components of an SD-WAN service
- ONUG – In 2019 ONUG has changed its mission with regards to SD-WAN standard, it decided not to work on an SD-WAN protocol standard but focus on the orchestration level for integrating SD-WAN connectivity into hybrid multi-cloud environments

Since there is a need for an SD-WAN protocol standard and since it does not look like this will be done by one of the standards bodies, the other option is for a solution to become the defacto standard. An open-source solution such as the one from flexiWAN is one path to this. An SD-WAN overlay protocol would be a combination of IPsec plus VxLAN, plus an additional field for vendor specific logic.

What is an SD-WAN open source & what is the difference between “open” and open source?

Most if not all SD-WAN companies make use of open-source components in their products. They then typically add proprietary code they developed along with some sub-licensed 3rd party building blocks and create their closed code SD-WAN product from it. Some SD-WAN vendors do offer APIs to perform specific functions, for example, to automate provisioning and configuration of edge devices, this does not make these SD-WAN solutions open or open source.

More on what is an SD-WAN open source

An open-source SD-WAN would offer its code to be available at some public repository such as GitHub or GitLab. As an example, flexiWAN is available on GitLab. The other part of being open source is the license available for using the code, naturally, companies that offer complete products as open source also need a way to generate revenue otherwise, they will not exist but there should be an option for users to take the code, compile it and use it under the terms of the opens source license.

What is an open SD-WAN product?

As mentioned earlier in this section, some SD-WAN vendors offer APIs in their SD-WAN product, mainly for provisioning automation and configuration. This does not make these products open. The typical SD-WAN architecture vendors follow is bundling many technologies and features in one large software stack. This architecture prevents feature flexibility and the option to include technologies of other vendors in the deployment. It imposes a take it or leave it approach where the complete stack needs to be deployed with no option for differentiation for the service provider. An open SD-WAN product would include a networking foundation

layer that allows to extend its capabilities with technologies of different vendors. flexiWAN offers this capability though its application framework and by that is the world’s first SD-WAN application store.