Sangfor SD-WAN White Paper

Sangfor Technologies Co., Ltd.

October 15, 2018

Copyright Statement

Disclaimer

Feedback

For any suggestions, please contact us by any of the following means:
Address: Block A1,Nanshan iPark,No.1001 Xueyuan Road,Nanshan District,
Shenzhen,Guangdong Province,P.R.China(518055).
Hotline: +60 12711 7129 (7511)
Email: sales@sangfor.com/marketing@sangfor.com
Latest technology and product information is available at the official website of SANGFOR:
www.sangfor.com.

SANGFOR

Contents

Chapter 1: Preface

In recent years, as a new technology in the network field, SD-WAN has been developed rapidly in various industries. The acceptance for SD-WAN by enterprises is increasing, and the major vendors have also put forward their SD-WAN solutions.

However, the awareness to SD-WAN is not the same: SD-WAN vendors have their own ideas and competed without cooperation which resulted that the proposed solution cannot form a unified standard, which was not conducive to the O&M and coordination of network as well as the promotion of technology itself. So, what exactly is the SD-WAN? What are the main scenarios and technical advantages of SD-WAN?

This white paper introduces current problems confronted by the traditional WAN architecture to raise the background of SD-WAN occurrence, introduces what is SD-WAN, explains the functional characteristics of SD-WAN architecture in detail and summarizes the values and market prospect of SD-WAN. Then, it summarizes the main scenarios and typical cases of SD-WAN and lastly, proposes the development trend of SD-WAN.

Chapter 2: Challenges Confronted by the Traditional WAN Architecture

Compared with the past, the management and maintenance of enterprise WAN (Wide Area Network) are becoming more and more complex and expensive. At the same time, enterprises become increasingly dependent on the long deploy period of network. Some enterprises even require the WAN to run uninterruptedly for 7 * 24 hours (new retail and unmanned retail scenario). This has led to fewer and fewer time for enterprise network teams to adjust their network. From this we can see that the production and efficiency of the enterprise branches are limited by many factors of the traditional enterprise WAN:

1. Branches have long online cycles and high online costs (traditional architecture which uses MPLS)

The MPLS online cycle is quite long and it will be even longer if the branch location does not have the resources of ISP. SD-WAN architecture does not have this problem because SD-WAN can use any link for network transmission.

In addition, in the traditional WAN architecture network, devices (routers) have complex configurations, which require professional IT engineer.

2. The structure of traditional WAN is complex and is difficult to maintain. The efficiency of troubleshooting is relatively low in case of issues.

To reduce cost, branch sites do not have professional IT engineer. Therefore, when the remote branches have WAN issues, IT managers cannot discover the issues in time. At the same time, in the process of locating the issues and troubleshooting, the means that can be used are very limited and inefficient.

The use of full redundant architecture in the enterprise branch network is a common way to effectively cope with the above problems in the traditional WAN architecture to ensure the high availability of the enterprise branch WAN. However, it requires that the branches are equipped with a backup link and a complex configuration on the router so that the backup link is automatically switched in case of faulty on the main link. The link backup in main-backup link causes multiple increase in the cost of the branch links, but the utilization rate is very low, which is quite wasteful.

Conclusion: The traditional enterprise WAN architecture made the network management team spend considerable energy in ensuring the availability of network connections and recovering branch network failures. But they are unable to pay attention to the use of WAN specified business and cannot innovate the business, such as matching the corresponding network resources and energy according to the importance of business and benefits.

3. The growing security demands of branch network increase the cost for security products.   However, the more complex the network topology, the more difficult to maintain the branch network. As a result, the enterprise invests more costs in the branch network, but cannot clearly perceive the output (whether the branch network becomes more stable or not).

4. The construction and maintenance of traditional VPN network are very complex. PCI (Payment Care Industry) security regulations require that the transaction data transmitted within the enterprise LAN must be transmitted by encryption rather than in clear text. Therefore, most enterprises will use VPN for the secure networking during construction of enterprise branch WAN. Yet, due to the point-to-point characteristic of traditional IPsec VPN, the construction of VPN network is very complicated. Considering enterprise branches are under large scale network scenarios, most enterprises will use the same VPN encryption key in all branches for the convenience of management. Thus, once a branch is controlled by an attacker, all branches in the enterprise WAN will be lost

Chapter 3: Definition and Features of SD-WAN

3.1 SD-WAN Definition

Software-Defined Wide Area Network (SD-WAN) is a service formed by applying SDN technology into WAN scenarios. This service is used for enterprise network and help customers reduce WAN costs and improve the flexibility of network connectivity.

3.2 SD-WAN Features

SD-WAN solutions have the following features:

(1)   Support real-time dynamic path selection based on application and network quality

Nowadays, most of the enterprise business have undergone a digital transformation which importance is self-evident. Business towards to cloud increase the importance of IT upgrades. As the network is a necessary channel for business access, network experience is getting more and more attention. In case of the network interruption or congestion, the office employees and the normal business operation of customer will be influenced. To ensure the availability of the network, enterprises will purchase several physical transmission links in branches, headquarters, data centers and so on. The traditional VPN can only use static configuration to fix the specific business on the specified link and does

not support the real-time monitoring of the link quality, which easily waste good quality link resources or leads to poor experience due to traffic congestion and easy to cause the unbalanced link usage.

The most important feature of SD-WAN is to build OVERLAY multi-tunnel link concurrently on UNDERLAY physical network and to monitor QOE (packet loss, delay, jitter and other parameters) of each line in real time and to carry out intelligent and detailed traffic scheduling based on the above. It needs to support the identification of customer services and able to adjust business priorities so that the important business is automatically assigned to the automatically identified quality links or link with fine resources. When the link is interrupted, it can be switched to the backup link within 1 second. When the link quality is insufficient to guarantee the experience of an application, it can be switched to other links automatically. These are the minimum basic requirements for SD-WAN intelligent routing.

(2) Support the independence of network transmission and virtualization of transmission resources

In the past, customers needed to buy expensive MPLS and other private lines to guarantee the network access experience which leads to not only high cost of bandwidth but also the long implementation cycle (several weeks even to months). Along with the constant improvement of the quality of Internet bandwidth, it has been a trend to use the Internet bandwidth to replace the private line wholly or partially. The physical network of SD-WAN may be a private line, Internet bandwidth.

To make full use of these transmission resources, SD-WAN products must be able to support multiple virtualized link as a large resource pool, just like CPU and the virtual pool for storage resources, and able to support the superposition of bandwidth and on-demand scheduling.

(3) Support the easy deployment of device plug-and-play

The implementation of traditional network devices, especially in multi-branch scenarios, is quite challenging for enterprises. IT engineer need to travel to the branch to provide support, which not only causes high costs but also a long implementation cycle. SD-WAN device must be able to deploy as simple as possible for plug-and-play. The device is all pre-configured at the central terminal and the branch devices do not need local complicated configuration after correctly plugging in the network at the branch.

Then, the devices can be connected to the centralized management devices to automatically download the specified configuration and policy to execute.

(4) Support simplification of multi-device management through centralized management, AutoVPN and other technologies

When the quantity of branch site is too large, the management and visualization of the multi-device will become critical. Without a unified centralized management system, it would be a disaster for IT manager. Because 1000 devices require 1000 times of remote logins and 1000 times of configurations, it is not only inefficient, but also extremely error-prone. By centralizing the management of products, you only need to configure the unified template and distribute to all branches to ensure the consistent configuration on all branches. The process will only take few minutes. At the same time, it is also very important to manage and visualize the virtual tunnel of the whole network. Managers need to know which applications use the bandwidth and which branches consume bandwidth, as well as which branches is off-line and alarms are located.

(5) Support Software-Defined Security

Most SD-WAN vendors only solve the connection problem and ignore the branch security construction. Because SD-WAN uses the Internet broadband to replace private lines, although it reduces the cost of links, although it reduces the cost of links, but the exit is vulnerable to attacks as it is opened for public. Therefore, it is not enough for a complete SD-WAN solution to merely solve the network connection problem, but the solution must also support integrated firewall, anti-intrusion and other security products. Perhaps the best solution is to integrate security features in SD-WAN device or import internet traffic to centralized security resource pool for traffic cleaning.

(6) Support simplified service distribution

Customer requirements may change dynamically regarding network connection and security issues. At the initial stage, maybe only solving quality problem connection is necessary, but it can dynamically extend the secure NFV when the security issue becomes more and more serious. This requires solutions to support dynamic scalability and genuinely achieve software-defined based on changes of customer requirements, arranging the branch NFV business from centralized management platforms and one-click distribution to specified branches, without travel to the branch site for installations.

3.3 SD-WAN Technical System

Combined with its own technical leadership in the security field, Sangfor SD-WAN proposed the safe and controllable SD-WAN products. By centralizing the management, it provides rapid deployment for branch sites in the deployment stage and policy centralized management and visual controllability for the whole network devices during the O&M stage. Through bi-directional link, real-time detection and path selection based on service, the best quality of business network can be guaranteed. Sangfor SD-WAN solutions provide the following capabilities:

3.3.1 Rapid Deployment

Sangfor SD-WAN make it possible for zero IT implementation and dynamic business adjustment through mail deployment. Customer only need to pre-configure the public network information and access to centralized management platform, then the information mail with be generated and sent to the branch user. Branch user only need to open and click on the mail link, then the deployment of the device can be completed.

3.3.2 Auto VPN

Combined with Sangfor patent VPN technology, Sangfor SD-WAN realizes the VPN network topology according to the VPN drawn and obtained from the headquarter centralized management platform to rapidly build a virtual private network for enterprise based on WAN network.

3.3.3 Dynamic Path Selection

SD-WAN needs to achieve link policy control at the application-level, such as business applications are prioritize to run on the best link while other applications have lower priority. Through real-time detecting the packet loss, delay, jitter of multiple links Sangfor SD-WAN puts forward the best routing scheme for different applications. Thus, customer can maximize the values of all WAN link bandwidth while the core business is guaranteed.

3.3.4 Centralized O&M

SD-WAN needs to monitor and display the whole network business situation based on real-time and able to support unified policy update for the whole network rapidly. By providing branch alarms and monitoring capabilities on the branch status, customers now finally get real-time experience of the business in time and support centralized problems solving in the headquarters in case of failure.

Chapter 4: The Values of SD-WAN

The goal of SD-WAN solutions is to replace leased line with Internet bandwidth and reduce the cost while enhancing the business access experience. So, a complete SD-WAN solution will include following values:

4.1 Reduce the Capital Expenditure (CAPEX) of Network Transmission Resources

By using Internet bandwidth to replace the leased line, the bandwidth and the availability of multiple links is better than single leased line. When there are many branch sites, the capital expenditure of link resources can be saved more than 50%.

4.2 Reduce Operating Expense (OPEX) during Deployment and O& M Stages

Through the plug-and-play deployment in the deployment stage, and the full visualization and unified management of whole network at the centralized management platform during the operation and maintenance stage, the customers' operating expense is greatly reduced, the management efficiency is enhanced and the cost for the network engineer in the branch office is also reduced.

4.3 Enhance the User Application Experience and

Security

With path selection and WAN optimization features, it can ensure that customer's core business applications run on the best link to guarantee its experience. Also, integrated security solutions via NFV and other means assures the protection of branch security.

Chapter 5: Development Status of SD-WAN

5.1 Development of SD-WAN

SD-WAN technology derived from Europe and America. The main background was that the multi-branch networking in Europe and America was built based on MPLS (more than 60 percent), the business was mainly in the customer self-built data center and the ISP guaranteed the quality of business to access network while the security was built centrally in the headquarters. With the popularization of the cloud service from the data center and SAAS, it was unrealistic to guarantee the quality by maintaining the use of connection from leased line to the cloud. On the other hand, the desktop cloud and the Internet apps occupied a large amount of bandwidth, so it was too expensive to use the leased line. The evolution of branch network and the use of hybrid WAN links to ensure the experience and distributed security of IT services became particularly crucial. The external environment for networking has made unprecedented changes in decades, promoting subversive innovation such as SD-WAN. After this revolution, may produce network giants such as New Cisco, so SD-WAN shows an explosive growth trend. Until now, the development of SD-WAN has experienced two stages:

SD-WAN 1.0 mainly solved the problem of how to guarantee the connection quality after using the Internet bandwidth by applying path selection, plug-and-play easy deployment, centralized management and visual controllability and so on;

In the era of SD-WAN 2.0, customer found that there are problems of branch site security and management problems. These problems were solved by security traffic clearing at the NFV in

branch office or drainage to the HQ for security cleaning, as well as supports online orchestration at the centralized management side and issuing services to the specified branch.

5.2 SD-WAN Market Survey

Although SD-WAN is a new network technology that has just been put forward for only 3-4 years, there are many indications showing that SD-WAN has developed rapidly. Many service providers have introduced new hybrid WAN solutions, and SD-WAN is the most popular solution. The SD-WAN market is growing rapidly, from the view and observation of industry consultants: research reports of Rayno Report indicated that more than $360 million of venture capital has been invested to SD-WAN startups. Gartner predicts that SD-WAN device sales will reach USD 1.24 billion by 2020 and the global market component growth rate will be 57.4% in 2016~2020. By 2018, the scale of SD-WAN services deployed by enterprises would increase from less than 1% in 2015 to 30%. IDC predicts that SD-WAN revenues would reach USD 2.3 billion in 2018, and the compound annual growth rate will increase by 69% to reach more than USD 8 billion by 2021.
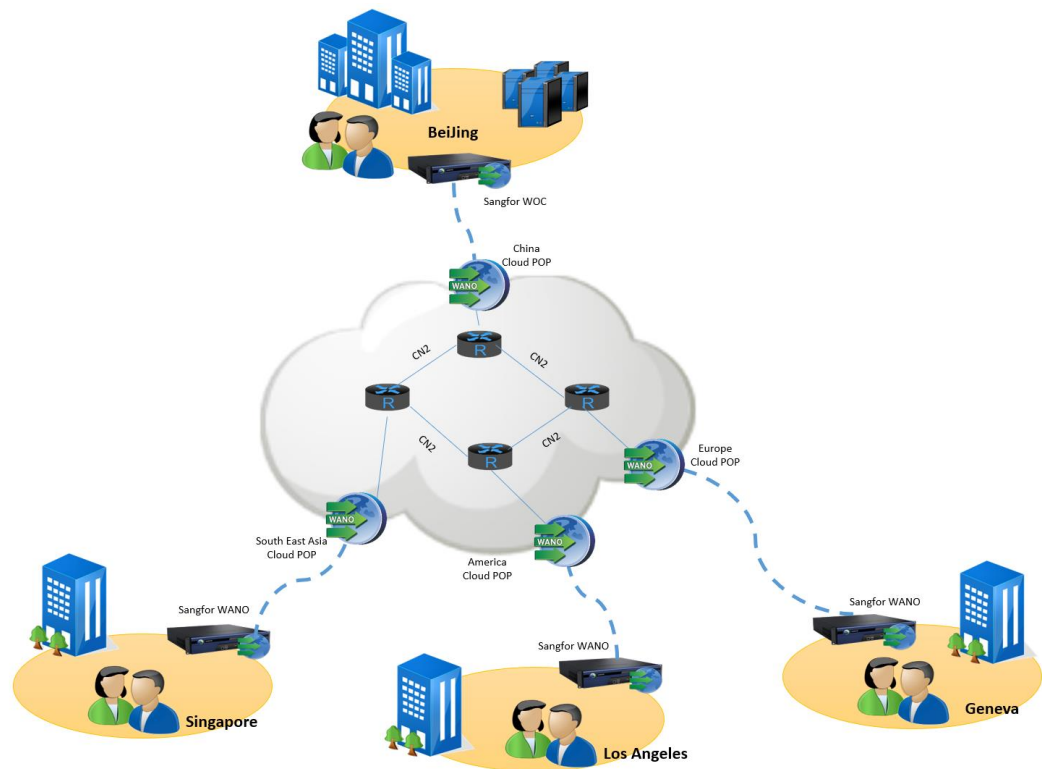
The market size of SD-WAN is expected to grow from USD 738.9 million in 2016 to USD 9.0663 billion in 2021, with a compound annual growth rate (CAGR) of 65.11 %, according to the survey report of MarketsandMarkets. North America remains to be a big market for SD-WAN, while China's market share remains between 20% and 25%.

Chapter 6: Main Scenarios of SD-WAN

6.1 Cloud Network

In this scenario, overseas sites (e.g. Singapore, Geneva, Los Angeles) do not need to rent expensive and inflexible leased lines from local ISP, but only need to buy local Internet link. Through vpn networking of Sangfor SD-WAN, each cloud POP node is connected while Beijing cloud POP nodes are connected by domestic data centers (e.g. Beijing) via Sangfor SD-WAN. A high-speed tunnel between cloud POP nodes is built through SD-WAN and CN2 backbone links to satisfy the needs of high-speed exchange visits between overseas office and Chinese datacenter. Meanwhile, it will lead to higher ROI and SLA in the leased line. For example, if it is necessary to visit the Beijing Data Center service from the overseas site of Geneva, the data from Geneva will

be transmitted to the Europe cloud POP node through Sangfor SD-WAN. The data from the Europe cloud POP node then will be transmitted to Beijing cloud POP node through the high-speed CN2 network, and the data from the Beijing cloud POP node will be transmitted to the Beijing data center. So, the link achieves low delay and 0 packet loss, which enables better visit experience.

6.2 Enterprise Branch Office Network

With the digitized transformation of enterprise business, the importance of IT construction has been enhanced, the experience for the branches to access to headquarter, management and regulation has been stressed by customers gradually. Reliability and security of traditional core services are ensured by the interconnection of leased lines, but the cost of the leased line is expensive and the deploy cycle is long. At the same time, the quality and capacity of internet bandwidth have been fully improved, so customers are motivated to replace some or all the traditional leased lines with internet bandwidth, especially for the small and medium-sized branches that need to develop business quickly. Since the traditional lines cannot support the rapid expansion of business, in this case, the key for future IT investment of

enterprises is how to use hybrid links to ensure the experience of the core business network.

Because of the complex configuration of the traditional VPN networking, each branch needs professional IT engineer to carry out daily operation and maintenance. With the rapid growth of enterprise business, The cost for IT O&M increase proportionally.

Through the fast implementation by mails, the path selection, the bandwidth management, centralized operation and maintenance control and other means, aiming at different sizes of branches, Sangfor SD-WAN provides targeted intelligent routing policy to ensure the optimal experience of the overall business and makes full use of the value of private lines as well as Internet bandwidth to meet the business rapid increase with less IT investment.

Chapter 7: Development Trend of SD-WAN

7.1 Interface Standardization

With the development of SD-WAN, each vendor strives to occupy the market rapidly, but interface standards of various vendors are not consistent, so it is difficult to coordinate and promote. In the future, SD-WAN will be developed to realize the interoperability among each vendor and standardized interfaces of devices.

7.2 Intelligent Management & Collaboration

SD-WAN will provide connections to users' terminals. To simplify O&M of WAN, artificial intelligence and machine learning will be introduced for path selection in the future. The network management will become more intelligent to ensure the robustness of WAN.

At the same time, users often need multiple vendors to strike a balance in SD-WAN deployment and do not want to be intervened by vendors. SD-WAN network development must get rid of the closed management system and achieve SDN collaborative control or business collaborative arrangement based on

multi-manufacturers. At the same time, SD-WAN service providers also need to strengthen the management of multi-tenant architecture to adapt to the business demands.

7.3 Security Integration

SD-WAN providers need to work more closely with security providers so that the SD-WAN platform will contain more embedded security functions that use advanced threat detection technologies, and the platform can integrate the next generation firewalls, unify threat management and has anti-virus functions. Therefore, users can deploy network security functions in branches, data centers or clouds to ensure that connection terminals of users and WAN are protected from ever more complex threats.