Current Trends in Using the Software-Defined WAN

Abdelfattah Mohamed

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, m.zaki178@gmail.com

Abstract. *The given work is devoted to the investigation the current trends of using the Software-defined WAN as a specific application of software-defined networking technology applied to WAN connections such as broadband internet, 4G, LTE, or MPLS. While connecting enterprise networks – including branch offices and data centers – over large geographic distances, SD-WAN simplifies the management and operation of a WAN by separating the networking hardware from its control mechanism.*

Keywords: *SD-WAN, broadband internet, enterprise network, cloud-based applications, network security.*

I. INTRODUCTION

SD-WAN consists of several technologies combined with newer improvements. Redundant telecommunication links connecting remote sites date back to the 1970s with X.25 links used for remote mainframe terminal access. Central management of those links with a greater focus on application delivery across the WAN started to become popular in the mid-2000s. SD-WAN combines the two, and adds the ability to dynamically share network bandwidth across the connection points. Additional enhancements include central controllers, integrated analytics and on-demand circuit provisioning, with some network intelligence based in the cloud, allowing centralized policy management and security.

Networking publications started using the term SD-WAN to describe this new networking trend as early as 2014. Software-defined WAN is quickly replacing traditional Wide Area Networks (WANs) as more enterprises realize the need to rethink networking for today's cloud-centric world. SD-WAN simplifies the way networks are designed, deployed and managed. It also brings powerful capabilities that increase the efficiency and agility of IT teams. In addition, SD-WAN devices can be installed without removing the existing network equipment and can be managed from a central console using a modern graphical user interface.

II. PROBLEM SOLUTION AND RESULTS

Considerable savings can be fulfilled by moving some or all traffic from MPLS to cost-effective broadband alternatives in a Hybrid WAN configuration. SD-WAN makes it easy to achieve cost savings by automatically splitting traffic between low-cost and highly-available WAN links based on business criticality. This is possible when the SD-WAN solution can identify traffic by application and steer it according to policy-based rules. While there is no doubt that cost savings is a key benefit of SD-WAN adoption, it's not always easy to recognize how much can you save and what is your true return on investment.

Software-defined WAN is making it simpler to set up and manage networks at branch offices despite their growing complexity and a lack of onsite IT staff. With zero-touch, rapid deployment, almost anyone can plug in an SD-WAN gateway and watch as it is discovered, provisioned, and brought online. One network engineer can administer dozens, maybe hundreds, of SD-WAN devices on an ongoing basis. This is made possible by policy-driven management, which translates business requirements into operational rules that are transmitted to all SD-WAN devices across the enterprise network.

Network performance is important for business-critical applications and unified communications – especially when applications run in the cloud. But not all network traffic needs to move quickly. Software-defined WAN combines traditional Quality of Service with the ability to steer the traffic of different applications and users onto appropriate paths. SD-WAN can also monitor the "health" of WAN links and automatically route traffic onto an alternate (backup) path when the primary path becomes congested. Nevertheless, that doesn't help if all available paths are bad. In this case, the WAN optimization can be used together with SD-WAN to improve performance across congested links and high-latency connections.

Software-defined WAN enhances **security** in several ways. SD-WAN can identify network traffic by source/destination, application, and users. Then it routes the traffic according to centrally-defined security policies that control access to zones and the Internet. SD-WAN gateways form connections between sites using VPN tunnels with advanced encryption. Many gateways come with a robust perimeter firewall that meets most security needs. Internet traffic that requires a firewall with advanced features can be backhauled through a central access point with stronger security or sent through cloud security provider.

III. CONCLUSIONS

It can be concluded that SD-WAN is used in connecting branch/remote sites directly to the Internet as the increasing reliance on cloud-based applications in most organizations is a driver for this use case. Setting up Internet break-outs from branch/remote offices is slow, inefficient, and error-prone when using traditional methods. SD-WAN drastically simplifies and speeds the process. You can quickly design a shadow appliance, which is a placeholder for a physical device, on the central management console. Then use zero-touch provisioning to bring the SD-WAN device online without the need for administrative action when it is plugged in at the remote/branch office.

REFERENCES

[1] G. Blokdyk. *Software-Defined WAN SD-WAN A Clear and Concise Reference*. 5STARCooks, 2018.

[2] G. Blokdyk. *SD-WAN A Complete Guide*. 5STARCooks, 2018.

[3] R. Naggi and R. Srivastava. *SD-WAN The Networking Blueprint for Modern Businesses*. Amazon Digital Services LLC, 2018.

[4] G. Blokdyk. *Sd-WAN and Security the Ultimate Step-By-Step Guide*. 5STARCooks, 2018.

[5] P. Goransson, C. Black, T. Culver. *Software defined networks: a comprehensive approach*. Morgan Kaufmann, 2016.