The Mandate to Adopt a Software Defined Branch Office

Ashton, Metzler
& Associates

Leverage Technology & Talent
for Success

Introduction

Today's most commonly used branch office WAN architecture started to be implemented around the turn of the century. This architecture calls for MPLS access at each branch office, typically running over T1or E1 links, and higher speed WAN access at one or more corporate data centers. In most cases, Internet traffic is backhauled to a corporate data center prior to being handed off to the Internet.

The primary reason for the popularity of the traditional branch office WAN architecture is that until recently there hadn't been a fundamentally new WAN technology or architecture introduced into the marketplace since the introduction of MPLS almost twenty years ago. That situation began to change a couple of years ago with the introduction of a new class of WAN solutions that takes a software-centric approach to providing WAN products and services. This new class of solutions is typically referred to as a Software Defined WAN (SD-WAN). The interest in SD-WANs was discussed in a recent article in Network World. According to that article, the SD-WAN market, which was valued at $225 million in 2015, is currently growing at a 69% compound annual growth rate and will be valued at $8.05 billion in 2021.

One of the primary reasons why there currently is so much interest in SD-WANs is because SD-WANs hold the promise of greatly simplifying the operations of the branch office WAN at a time when few network organizations are increasing the size of their staff. While simplifying the ongoing operations burden of the branch office WAN is an important goal, it is, however, only a starting point. The broader, more important goal is to simplify the ongoing operations burden that is associated with supporting all of the networking functionality within a branch office.

The operations burden associated with supporting branch offices results in large part from the fact that virtually all IT organizations have implemented branch office networking in a highly-compartmentalized manner. For example, within a branch office there are separate appliances to support each of the networks found in that office; i.e., both the wired and wireless networks within a branch as well as the WAN that connects branch office users to the external resources they need to access. The compartmentalized nature of branch office networking extends beyond just having separate appliances for each type of network. It also includes each branch office network having its own way to implement management and policy.

One goal of this white paper is to discuss some of the key industry trends that are making the task of managing and securing branch office networks increasingly more difficult. Another goal is to discuss how, similar to the situation in the WAN, the optimum way to drastically reduce the operational burden associated with the branch office is to adopt solutions that take a software-centric approach to providing all of the branch office networking functionality. This new class of solution is referred to as a Software Defined Branch Office (SD-Branch Office).

Factors Driving Change

Several factors are making the current approach to the implementation and ongoing management of disparate branch office networks unsustainable. Those factors include the:

- Large and growing adoption of cloud computing;
- Large and evolving adoption of mobility;
- Burgeoning adoption of the Internet of Things (IoT);
- Growing use of the Internet as part of a hybrid WAN.

Cloud Computing

A recent article in Forbes quantified how the use of cloud computing has grown over the last several years and how it is expected to grow over the next few years. According to that article, "Cloud computing spending has grown at 4.5 times the rate of IT spending since 2009 and is expected to grow at better than 6 times the rate of IT spending from 2015 through 2020." The article added that "Worldwide spending on public cloud computing will increase from $67B in 2015 to $162B in 2020 attaining a 19% CAGR."

The growth of cloud computing presents IT organizations with a couple of challenges. One challenge is that in many cases a company's business unit managers bypass their IT organization and acquire services directly from public cloud providers. To respond to this challenge, IT organizations must avoid having a *not invented here* culture and instead they must act as honest brokers to determine which functionality is best provided internally and which functionality is best acquired from a cloud computing provider.

Another challenge associated with the growth of cloud computing is that even if they are involved in the choice of which cloud based solutions are adopted, network organizations end up with very limited visibility and control over those solutions. As a result, organizations face an unacceptable choice. They can continue to adopt public cloud solutions and hence enjoy the agility and cost savings that are associated with those solutions. However, in the current networking environment adopting those solutions means that the organization will lose insight into the performance of those cloud-based solutions and they will also lose the ability to troubleshoot problems.

Mobility

A recent article discussed mobility and concluded that a number of trends are causing enterprises to adjust their operations in order to account for the growing use and demand that is associated with an increasingly mobile workforce. One trend that the article discusses is that similar to the BYOD movement, employees are driving another movement - the movement to "Bring-Your-Own-Application" (BYOA). BYOA refers to employees bringing applications that they use on their personal devices, such as Dropbox and Google Docs, to work. According to the article, the use of employee-founded applications is becoming prevalent and is creating even more security vulnerabilities that were created by the BYOD movement.

Another trend the article discusses is that organizations will need to support a growing number and a greater range of devices. According to the article, the global mobile workforce is set to increase to 1.87 billion people or 42.5% of the global workforce in 2022, up from 38.8% in 2016. In addition, as workers become increasingly mobile, so does their primary work device. As a reflection of this trend, the article stated that employees are moving toward smaller, more portable devices and tablets as well as wearables and ultrabooks.

The combination of BYOD, BYOA, and the growing number and types of devices means that the security challenges associated with mobile office workers will continue to grow and evolve significantly over the next few years.

The IoT

In a report published in early 2017, Gartner forecasted that 8.4 billion connected things will be in use worldwide by the end of 2017, up 31 percent from 2016, and that there will be 20.4 billion connected things by 2020. As discussed in a recent blog, the IoT impacts every industry with business-critical use cases being developed in many verticals including retail and healthcare.

The financial services industry is another vertical that is predicted to be heavily impacted by the IoT. The Deloitte Center for Financial Services was quoted in an article as saying that, “By enabling the collection and exchange of information from objects, the IoT has the potential to be as broadly transformational to the financial services industry as the Internet itself.” According to that article, some branch-based examples of IoT-based applications include video tellers and kiosks in bank branches where sensing technology can monitor and take action on the consumers’ behalf. In addition, mobile geolocation capabilities combined with beacon technology can ‘introduce’ a customer upon entering a branch with pre-queuing for improved service. Unfortunately, the article also states that because of the combination of the increased use of the IoT and the requisite digital connections, that security vulnerabilities are likely to expand exponentially.

The Increasing Use of SD-WANs

As noted, the traditional branch office WAN architecture calls for MPLS access at each branch office and it also calls for Internet traffic to be backhauled to a corporate data center prior to being handed off to the Internet. Unfortunately, since the Internet traffic traverses the organization’s MPLS network prior to being handed off to the Internet, this approach increases cost and it adds to application delay.

As was also noted, there currently is significant interest in SD-WANs in part because SD-WANs hold the promise of greatly simplifying the operations of the branch office WAN. Because they enable dynamic load balancing of traffic over multiple WAN links, SD-WANs also hold the promise of enabling network organizations to cut cost. Network organizations cut cost by reducing or eliminating their use of relatively expensive MPLS circuits and providing the necessary WAN bandwidth via relatively inexpensive Internet bandwidth. Unfortunately, SD-WANs present network organizations with two critical challenges. One challenge is that managing traffic that is dynamically load balanced over disparate WAN services is notably more complex than managing WAN traffic that traverses a single WAN link or WAN trunk group. The second challenge stems from the fact that the reason that network organizations backhauled Internet traffic was to enable network organizations to secure this traffic in a centralized, easy to administer fashion. Network organizations won’t be able to add Internet links at branch offices, and hence cut the cost of their WAN, unless they can solve the operational challenge of how to easily manage and secure these links. However, as noted in the introduction, while simplifying the operations of the branch office WAN is an important goal, it is only a starting point. The broader, more important goal is to simplify the operations of all the networking functionality within a branch office.

A Software Defined Branch Office

As discussed in the preceding section of this white paper, the issues that are making the task of managing and securing branch office networks increasingly more difficult include the:

- Loss of visibility into the performance of cloud based solutions and the corresponding inability to troubleshoot related problems;
- Growing and evolving security challenges associated with mobile branch office workers;
- Growing and evolving security challenges associated with the use of IoT based applications within branch offices;
- Complexity that is associated with having a highly-compartmentalized approach to branch office networking in general and the complexity that is associated with managing an SD-WAN in particular.

One of the reasons why taking a software defined approach to WAN services provides so much value is because a central tenant of being software defined is that the control and forwarding functions are separated and the control function is centralized. This separation allows for a number of benefits such as policy-based routing and the ability to manage all of the network elements from a central site.

In line with the general concept of being software defined, a critical component of a software-defined branch office is that all the management functionality is centralized. Given the broad and expanding use of cloud computing, it is highly desirous to have the centralized management functionality be cloud-based.

Other key components of a software defined branch office include:

- Single policy to centrally administer the wired LAN, the wireless LAN and the WAN
    - Branch office operations are complex and expensive, especially as organizations manage traditional network components in different operational silos. By applying network controls through software, it’s possible to replace the need for separate configurations with the ability to administer centrally via a simple, common policy.
- Dynamic ability to route and optimize traffic over existing broadband and private WAN links

- The ability to easily onboard new users
    - Organizations are seeing rising costs and increasing delay associated with onboarding mobile users and IoT devices in a distributed architecture. A seamless onboarding experience allows faster provisioning which reduces both cost and gaps in service.
- There is application awareness and the provision of quality metrics for real-time applications;
    - Greater visibility and control over different business applications provides benefits across all aspects of branch networking, especially relative to improving the user experience and Quality of Service from RF to WAN (initial point of contact to the offload).
- There is sophisticated security functionality;
    - The traditional notion of a network perimeter no longer applies in a mobile and cloud networking model. Users and devices inherently access and communicate corporate data outside of the physical premise, in favor of dynamic access to resources on-the-go.
- There is role-based visibility and control down to the level of users and devices;
    - Leverage the insights and intelligence that the network access layer can provide to the WAN, such as context awareness and behavioral patterns of users, devices, and applications relative to location. If one branch is seeing a rise in cloud storage usage, automatically apply QoS based on IT priorities.
- There are a broad range of subscription-based and cloud-managed services available.
    - The trend of IT regaining control of the WAN signifies a change in overall branch architecture. SD-WAN delivery models pave the way for immense disruption in decades-old WAN infrastructure, which can be used to change the model of access layer networks for easier management and deployment.

Summary

There is no doubt that SD-WANs provide value in part because they ease the ongoing operations burden that is associated with the branch office WAN. There is also no doubt that adopting an SD-WAN is just a starting point towards achieving a more important goal. That goal is to simplify the ongoing operations burden that is associated with supporting not just the WAN, but all the networking functionality within a branch office.

Several factors are making the current approach to the implementation and ongoing management of disparate branch office networks unsustainable. Those factors include the:

- Large and growing adoption of cloud computing;

- Large and evolving adoption of mobility;
- Burgeoning adoption of the Internet of Things (IoT);
- Growing use of the Internet as part of a hybrid WAN.

In order for network organizations to respond to the factors identified above, network organizations need to adopt software defined branch office solutions. A key component of such solutions is that all the management functionality is centralized, preferably in the cloud. Other key components of a software defined branch office include:

- The wired LAN, the wireless LAN and the WAN are all part of a single network with a single policy that is administered centrally;
- The ability to dynamically route and optimize traffic over existing broadband and private WAN links;
- The ability to easily onboard new users;
- There is application awareness and the provision of quality metrics for real-time applications;
- There is sophisticated security functionality;
- There is role-based visibility and control down to the level of users and devices;
- There are a broad range of subscription-based and cloud-managed services available.

It’s possible for a vendor to develop a software defined branch office solution by making minor changes to their existing solution. It’s also possible to develop a solution that makes minimum use of the cloud. However, the most valuable solutions will be the ones that are designed from the ground up to be cloud-based and to fully leverage the advantages of a software-centric approach to providing branch office functionality.