FORTINET

What To Consider When Evaluating SD-Branch Options

Table of Contents

Executive Overview

The distributed enterprise (remote branches with a centralized headquarters and data center) is a common architecture for both public and private businesses. The adoption of multi-cloud architectures as well as Software-as-a-Service (SaaS) is causing these types of businesses to rethink their approaches to their network.

With more traffic flowing out of the network, advances in wide-area networking (WAN) technologies are offering improved user experiences and business outcomes. As businesses adopt these new WAN technologies, they are additionally taking a broader approach to the enterprise branch, looking for solutions that address the challenges faced at the branch as a whole. In addition to WAN efficiency, these challenges include:

- Complexity
- Security
- Cost

“As SD-WAN deployments grow, the market gradually transitions to software-defined branch and more holistic management of edge network security.”[1]

Section 1: Challenges at the Enterprise Branch

The traditional hub-and-spoke branch model that many distributed enterprises use can be challenging for a centralized IT staff to deploy and support. Core business-supporting technologies, such as WAN, security, and wired and wireless networks, are rarely integrated. Often multiple vendors and solutions are put in place, each with their own hardware and operating systems to manage. Meanwhile, performance requirements continue to rise due to cloud-based business applications (SaaS) and an increase in the number of devices connecting. These factors are straining traditional local-area networks (LANs) and WANs.

Legacy WAN Solutions

- Traditional WAN solutions are expensive and can also create performance bottlenecks that impact user performance and productivity across the business.
- Traditional WAN routing is not intelligent and cannot be assigned by policy to the right broadband channel.
- Failover options for traditional WAN systems have not been reliable, which can disrupt business continuity and affect productivity.

Complexity

- Management of LAN and WAN technologies that rely on multiple consoles and operating systems require significant cross-training and expertise to support.
- Without full visibility in a single location, IT staff cannot understand where issues are occurring. The result is that issues take too long to resolve, impacting productivity.
- Long deployment and provisioning times are common as IT staff members struggle to coordinate LAN edge and WAN edge technology rollouts.
- Complexity also extends into product licensing. Often each solution, whether single or multivendor, has licensing that needs to be maintained and monitored.

Security

- Most traditional distributed enterprise branches relied on centralized security, where traffic is backhauled through the data center for inspection. The shift to cloud technologies drives the need to secure both the WAN and LAN edges in a distributed manner to avoid quality of experience (QoE) issues when traffic is routed first to a corporate data center.
- The introduction of business-enabling technologies in the form of Internet-of-Things (IoT) devices has significantly increased. There is a need for visibility to catalog and secure these devices at the remote branch.

High Costs

- The current industry trend of implementing licensing on every aspect of a solution has created additional financial considerations for IT administrators and VPs as they try to support critical use cases. Often multiple aspects for securing the LAN and WAN edges require licensing that is expensive and complex.

Section 2: Six Things To Consider When Evaluating SD-Branch Options

Digital transformation initiatives deliver better customer satisfaction and improve employee productivity, but they also create new network edges that need to be secured.

How do you build a secure, agile, and resilient branch architecture that takes advantage of the latest technologies while reducing cost? Secure SD-Branch solutions look to answer this question by combining network security with LAN and WAN functions. They include software-defined WAN (SD-WAN), routing, integrated security, and centrally managed LAN/Wi-Fi functions in one hardware platform.[2]

These solutions improve performance and manageability of the remote branch while reducing cost and complexity. Following are six key factors that decision-makers should look for when considering SD-Branch for their organization:

1. Technology integration
2. Management and deployment agility
3. SD-WAN performance
4. Security
5. Address IoT
6. Total cost of ownership (TCO)

Technology Integration To Reduce Appliance Sprawl

Any approach to creating an efficient, secure, distributed enterprise branch is hampered if the key technologies are not integrated. An integrated solution will simplify and reduce workloads on resource-challenged IT teams.

SD-Branch solutions can reduce complexity through the consolidation or convergence of key features. The resulting platform will simplify the branch architecture, making it easier to support and manage. In addition, with better integration of security along with LAN and WAN platforms, IoT security can be better addressed.

Centralized Deployment and Management To Simplify Operations

Centralized deployment and management is foundational in today's distributed enterprise environments. An effective SD-Branch solution provides tools to centrally deploy and manage key LAN and WAN edge functions so no specialized IT expertise is required at the branch. Organizations can increase agility through fast provisioning, streamlined configuration, centralized monitoring, and support. Zero-touch deployment saves time and money by reducing costly truck rolls to support remote deployments.

“The most compelling argument for SD-Branch is operational agility.”[3]

Secure, High-performance SD-WAN

Given the issues (noted above) with traditional WANs, enterprises need a replacement infrastructure with significant simplification, an improved cost advantage, and better support for new multi-cloud and SaaS-based business models.

Since one of the great benefits of SD-WAN is direct internet access, security must be comprehensive and powerful. With more than 87% of web traffic encrypted, security at the branch must be able to check for hidden threats without impacting network performance.[4]

As core applications move to the cloud, SD-WAN must be **application aware**. This enables monitoring and management of traffic patterns, balancing bandwidth, and scaling performance across the enterprise.

However, identifying an application is only the beginning. An effective SD-WAN must include **path awareness intelligence** to intelligently route and prioritize applications to drive successful business outcomes.

With cloud connectivity critical to the distributed enterprise, multi-broadband support **for WAN resilience** becomes a core requirement as well. The ability to monitor and assess multiple WAN links in real time and offer WAN path remediation and per-packet steering is also key.

> **“Today, 90% of SD-WAN solutions do not have security and network pieces integrated; organizations typically must buy and manage them separately.”[5]**

Effective, Integrated Security Across WAN and LAN Edges

An SD-Branch is most effective when security is integrated at the beginning of the process and not layered or bolted on afterwards. A solution that is designed within an integrated framework reduces complexity and provides better security.

- **Next-generation firewall (NGFW)** security is a key requirement for enabling direct internet access in an SD-WAN architecture. At the LAN edge, NGFW protection is critical for reducing risk exposure across an extended network. NGFW security should be integrated into the LAN and WAN edge to create policies that can be monitored and enforced from the end-user through the LAN and to the WAN interface. A single-box solution that combines both network and security functions can strengthen protection across the distributed environment while simplifying controls and reducing investment costs.
- **Network access control (NAC)** is the key to visibility. It is difficult to secure the LAN edge if you do not know what is connected to it. Security cannot be taken for granted as hackers will seek out the weakest places in your network architecture to exploit. The ability to see and understand the users and devices utilizing branch services is needed to implement policies at both the LAN and WAN edge.

Securely Address IoT

IoT devices continue to proliferate and attract cyber criminals due to the often lax security of the onboard operating systems. With device-level visibility and secure, automated onboarding of IoT, NAC addresses this. NAC deployment can be expensive and time-consuming. Therefore, a key consideration for an SD-Branch solution needs to be how NAC technology is enabled at the LAN edge. NAC should be able to be centrally managed, and licensing should be simple and cost-effective (if not free).

It has been predicted that in 2020, 93% of enterprises and 80% of industrial manufacturing companies will adopt IoT technology. Globally the same report estimates the installation of 31 billion IoT devices worldwide.[6]

Compelling Total Cost of Ownership (TCO)

Cost can be a decisive factor in determining which is the best SD-Branch solution for your organization. Short-term costs are easily established by a product and services quote. Long-term TCO can be harder to establish but is key to making the right decision. While hardware costs are typically one-time costs, licensing and support costs can make up the majority of the long-term cost associated with a solution.

Unless you are considering a managed service, the cost of the WAN links is fixed regardless of vendor, but how those links are utilized can have large impacts on operational cost. It is therefore important that the SD-WAN component of your SD-Branch solution can make weighted decisions on which link to use when (path awareness intelligence).

Licensing and support costs loom large both in cost and complexity. The list of required licensing for an SD-Branch solution should be short and easy to understand.

Management operations and support costs are also a large component of TCO. A solution that has security and network control functions integrated into a single pane of glass reduces complexity and simplifies management. Security staff can spend less time managing the various aspects of network and security operations and correlating events.[7]

IDC predicts that up to half of the SD-WAN market will evolve into the SD-Branch market by 2024 as SD-WAN vendors add additional network, security, and management functionality to their SD-WAN platforms beyond routing connectivity.[8]

Summary

As the move to multi-cloud architectures and SaaS reshapes the enterprise branch, companies harvesting the cost savings of SD-WAN are looking at extending some of those benefits to the LAN edge with an SD-Branch solution. An effective solution will reduce complexity while improving operational agility.

There is a crowded field of vendors offering SD-Branch solutions that vary widely in capabilities. VPs of Networking and decision-makers should carefully review the list of considerations above to ensure they are looking at a comprehensive, secure solution.

Fortinet Secure SD-Branch security-driven networking offers an accelerated convergence of networking and security. It provides a consolidated solution for SD-WAN, security, and LANs (both wired and wireless LAN) into a single proven secure platform. This provides simplified management, reduced overall branch complexity, and industry-leading security capabilities without complex licensing requirements.

[1] Brandon Butler, et al., "Five Key Enterprise Networking Trends to Watch in 2020," IDC, April 2020.

[2] Lee Doyle, "SD-Branch: What it is and why you'll need it," Network World, January 23, 2018.

[3] Ibid.

[4] Ken Xie, "The Power of Custom Security Processing," Fortinet, November 4, 2019.

[5] "What to Consider When Evaluating Your SD-WAN Options", Fortinet, September 12, 2019.

[6] "The IoT Rundown For 2020: Stats, Risks, and Solutions," Security Today, January 13, 2020.

[7] "What to Consider When Evaluating Your SD-WAN Options," Fortinet, September 12, 2019.

[8] Brandon Butler, et al., "Five Key Enterprise Networking Trends to Watch in 2020," IDC, April 2020.

FORTINET®

www.fortinet.com

784770-0-0-EN

October 31, 2020 9:54 AM

eb-evaluating-sd-branch-options