riverbed

Key Requirements for SD-WAN

Rethink Networking for the Cloud Era

Executive Summary

Digital transformation is happening now, and fast. It includes cloud, services, mobile. It's hybrid, it's the Internet, it's the user. Most importantly, it's the seamless orchestration of all these things *together.*

> **True digital transformation is the ability to orchestrate apps, networks, and devices to provide seamless access to digital services for end-users.**

Such orchestration can only be achieved by the one thing that connects everything: the network. In the highly centralized, controlled, and self-contained enterprise IT environments of the past, static hardware-based networking worked ok. But today, apps are both on-premises and in the cloud. Networks are both private and public. Users are mobile as well as remote. IT is more distributed, fragmented, and dynamic than ever. Taming this chaos of hybrid apps, hybrid networks, and mobile users demands a new approach to networking based on *policy automation* and *real-time orchestration* of all components of connectivity and access. That new approach is software-defined wide area networking (SD-WAN).

This is a period of significant growth for SD-WAN as we move past the initial hype phase. Many companies have done pilot projects and proofs-of-concept and are now moving to enterprise-scale. With successful large-scale deployments, SD-WAN is becoming a trusted technology critical to maximizing the value of the cloud. Not surprisingly, the growing market has attracted upwards of 20 vendors, from global players to start-ups. Software-defining networks allows both the disaggregation and aggregation of virtualized network functions, so telcos are also getting into the act as managed service providers offering bundles of these capabilities.

As you look across this crowded space—at the vendors, the service providers, the range of solutions with all their marketing claims—how do you choose? What are the requirements and capabilities you need in an SD-WAN solution that will drive maximum success for your business?

Creating an enterprise-scale software-defined connectivity and orchestration fabric requires the ability to:

- **Manage centrally** from a cloud console with a complete view of the connectivity fabric that unifies all enterprise networks, from the hybrid WAN at branch locations, into cloud infrastructure environments and even reaching to the end user with branch wireless and wired LAN networks.

- **Orchestrate globally** with business-aligned policies that automate enforcement of performance objectives and access privileges for all apps/users, wherever they may be.

- **Deploy remotely** with zero-touch activation of on-prem network components, and "one-click" extension into cloud networks.

These are the three essential requirements of an SD-WAN architecture which this paper explores in detail.

The Ability to Manage Centrally

Challenge Considerations

Improving agility in the midst of complexity. The pressure on IT organizations to quickly deploy sites, roll out applications, manage changes, and ensure seamless application performance across the enterprise is the highest it's ever been, and will only continue to grow.

At the same time, the complexity of the hybrid environment in which IT must assure end-to-end security, performance, and visibility is the highest it's ever been, and will only continue to grow.

Moving datacenters, applications, and storage to the cloud are all critical steps on the path to digital transformation. Now, enterprises need to bring the same cloud-grade agility to networking that they are achieving with cloud-based apps (SaaS) and infrastructure (IaaS). And they need the same level—or better—of performance that they used to get from on-prem apps delivered over private corporate networks.

Streamlining distributed deployment and operations. Businesses' approach to networking, however, hasn't evolved as quickly as other IT elements. Legacy networks continue to be hardware-bound, hard-coded, inflexible, and error-prone. The prevailing management model is decentralized. Routers are manually deployed in the field, a time- and labor-intensive effort with engineers entering arcane CLI commands at branch router interfaces. And at the branch, employees who are not IT professionals are often tasked with installing local network devices, firewalls, etc. In this old-school world, network changes take months, errors are frequent, links are often compromised, apps often slow, end-user experiences often poor.

Gaining visibility into and control over SaaS apps. Shadow IT—the ad hoc use of applications without organizational approval—makes application management even more challenging, and it is on the rise as employees seek better solutions than what their company provides to get their work done. Since bandwidth is now more readily available and more affordable, the adoption of SaaS and cloud apps can happen so quickly that IT teams do not even know what applications are in use or who is using them. They also have less visibility into end-user experience and little ability to manage the infrastructure and control application performance. Moreover, the majority of applications crossing the network are encrypted, which masks application identity, further complicating the ability to discriminate between business-critical and recreational traffic. And yet IT is responsible for ensuring the performance of all these applications for every user.

Automating path steering for hybrid networks. As network traffic continues to increase—caused by the growth of the sheer number of apps we all depend on, together with the universal use of bandwidth-intensive applications such as video and real-time collaboration— the demand for bandwidth continues to increase at a high rate. For cheaper capacity, enterprises have added Internet broadband links to their existing MPLS networks. According to IDC, 40-60% of enterprise data traffic is migrating from private WANs to the Internet. This creates a hybrid networking situation, increasing complexity and the need for automatic path selection.

Legacy approaches to networking can't cope with the complexity of the environment, volumes of traffic, or dynamic execution of business policy. Path selection requires visibility into the app, the network, and the destination. Use of Internet broadband as a transport for corporate connectivity also can make app performance and end-user experience unpredictable, impacted by additional jitter and packet loss as apps are delivered across public networks, so you also need instant and perfect visibility into the quality of every available path. Thus, for automation of path steering based on business policies to work correctly requires intelligent and instant correlation of metrics based on real-time visibility by the SD-WAN system into the desired destination of the application, its performance, the end-user experience of using the application, and the quality of available networks in between.

Improving application performance at the branch. The negative impact of latency and bandwidth issues on application performance and end-user experience are magnified by the proliferation of remote offices and branch offices (ROBOs) and mobile users, which radically changes network access and traffic patterns. Almost 80% of enterprise employees and contractors now work from ROBOs and access critical business services via the WAN, pushing bandwidth requirements well beyond initial design parameters. To solve these latency and quality issues requires that disparate networks be unified and optimized for seamless performance across the enterprise—for on-premises and cloud-based applications and services alike.

SD-WAN Requirements

The requirement for network management going forward is that it can be performed *centrally via policy* using a pane of glass that provides a *comprehensive view* of your enterprise connectivity fabric that connects datacenter and cloud apps with branch and mobile users, all in an integrated management platform that spans and unifies hybrid WANs, cloud networks, and branch wireless and wired LANs with a single policy framework.

To achieve this goal, the central SD-WAN orchestrator must:

☐ Support business-aligned policy through the use of simple, plain-language instructions based on a new set of primitives—apps, users, locations, performance SLAs, and security constraints—that correspond to the real world of business rather than the technical aspects of routing, eliminating the need for technical translation, intermediation, and error-prone device-oriented configuration updates.

☐ Enable software-defined control across a unified network fabric that extends across cloud networks, WANs, and branch LANs/WLANs to ensure seamless, secure application delivery, controlled by business policies, from any point to any point.

☐ Provide intuitive, cloud-centric workflows that allow instant and elastic expansion of new network end-points without additional operational overhead, with *zero-touch provisioning to remote locations* and automated *"single-click" expansion of connectivity and orchestration into cloud* environments.

☐ Automate creation of secure and encrypted inter-connectivity (VPNs) between datacenters, remote locations, the cloud, and end-users.

☐ Enforce performance and security control based on policy defined in the central management console.

The Ability to Orchestrate Globally

For today's hybrid enterprise, an effective SD-WAN solution must apply the power of software-defined and business policy-based orchestration across the entire connectivity fabric, spanning hybrid WANs, cloud networks, and branch wireless and wired LANs.

Challenge Considerations

Instantly provisioning into the cloud. Given the elastic and on-demand nature of IaaS offerings, SD-WANs need to be instantly connect-able to the cloud. This requires the ability to automatically provision gateways into cloud platforms and enable automated full-meshed connectivity between virtual private clouds (VPCs) and on-premises locations. The simplest, fastest solution is a one-click extension of the WAN to IaaS locations in a secure and optimized fashion, with the delivery of secure SD-WAN gateways and WAN optimization fully automated.

Securing, optimizing, troubleshooting SaaS apps. SD-WANs need to enable total management of SaaS applications from local breakout management, to latency mitigation, to visibility into end-user experience. The application performance experienced by end users can vary significantly from one person to the next and between one app and another. Factors affecting application performance include:

• Physical distance from the end user to the application server, which is typically longer with cloud-based apps than on-premises apps;

4

- Added distance in the network path when SaaS traffic is backhauled through an enterprise datacenter or via low-cost but indirect routes on the Internet;

- Bandwidth constraints that slow large file transfers associated with certain SaaS apps;

- Health and performance of the end-user device.

You need to automatically select network paths and prioritize traffic by application, user, or location. And you need to troubleshoot application performance issues. To do both of these things, your SD-WAN solution needs integrated tools that give you visibility all the way from the end user to the cloud.

Optimizing app performance. In a recent survey conducted by IDC, respondents identified the top three capabilities of a next-generation SD-WAN solution as security, WAN optimization, and policy control/management. Management of performance requires an intelligent, closed-loop process where issues can be identified and corrected in real time. Application optimization is a key part of this.

Latency issues become more pronounced to users across greater distance. To accelerate the wide variety of enterprise apps in use, optimization must streamline any type of application as well as address a wide variety of standards-based protocols such as CIFS, HTTPS, MAPI, NFS, and SQL, to reduce the number of network- and application-based transactions across the WAN for faster response times and end-to-end throughput. Also critical is the ability to autonomously control bandwidth usage for incoming and outgoing flows according to QoS policy, to ensure that both inbound and outbound traffic is appropriately prioritized by business criticality.

Ensuring end-to-end visibility. Effective optimization of application flows over the SD-WAN requires a proper understanding of both available network resources and usage of those resources by individual applications and users. To ensure performance of business-critical apps, end-to-end visibility on application performance as delivered by the optimized network also becomes essential.

SD-WAN Requirements

The goal is to use business-aligned, policy-based automation to define quality of service and access privileges for all apps and users, combined with automated path selection, end-to-end performance monitoring, WAN optimization, and security.

To achieve this goal, your SD-WAN solution must include a range of innovations that solve the hardcore technical issues involved in global orchestration:

□ Automated and secure connectivity to and between cloud networks and to branch networks to minimize operational overhead in creating VPNs.

□ Seamless integration with critical network services such as end-to-end visibility and WAN optimization are required for optimum application performance across the entire system. SD-WAN, when coupled with WAN optimization, further improves performance and infrastructure efficiencies.

□ Efficient management of local breakouts with the ability to select traffic directed to local breakouts vs. central breakouts vs. cloud-based security brokers from the very first packet based on Layer 7 information.

□ Automated path control with the ability to path select based on application type, business priority, and path quality as determined by available bandwidth, latency, jitter, or packet loss. Business-relevant traffic is routed on the highest performing path with switches to path performed dynamically and automatically as needed.

□ End-to-end network segmentation with all aspects of the segmentation integrated into a single concept of "zones":

- Ability to segregate traffic based on applications defined at Layer 7.

- Ability to segregate traffic based on users with Active Directory Sync.

- Ability to segregate traffic across the WAN and into branch wireless and wired LANs using VLANs and Wi-Fi authentication.

5

The Ability to Deploy Remotely

With cloud-based apps, every user is remote. An effective SD-WAN solution must extend the enterprise connectivity and orchestration fabric from the central place of management to provide all users, whether employees, partners, or customers, wherever they are located, with easy, secure, high-performing access to the applications and data they need.

Challenge Considerations

Zero-touch provisioning. SD-WAN replaces high-touch manual and device-centric deployment and configuration of individual routers, where each new device typically generates cascading changes across the broader network that can take months of planning and careful execution. Instead, with SD-WAN you can design, deploy, and orchestrate networks from the cloud using centrally-managed policies. Zero-touch vs. high touch. Easy to change from a central pane of glass vs. device-centric configuration of routers in the field. Configured and tested before deployment vs. having CLI errors revealed by app failures during business production.

Integrating with existing network elements. Automated, zero-touch provisioning is especially critical as enterprises migrate from a few SD-WAN branch locations to thousands. To do this they will need, in addition to zero-touch provisioning at the branch, the ability to integrate with other WAN and LAN branch network elements, such as WAN optimization and network firewalls, *without* compromising an application-centric approach to policy-definition and orchestration.

Working with existing routers. The practical reality is that companies will move to SD-WAN at their own pace, the same as with cloud adoption. Some companies will want to replace branch routers with SD-WAN appliances while others will overlay deployment of SD-WAN solutions as an intermediate step. In addition, your SD-WAN solution must be able to co-exist both with sites that have not yet migrated to the policy-based network, and with branches with legacy routing that has not yet been de-commissioned. SD-WAN policy overlays should automatically integrate with existing routers, WAN optimization appliances, and other existing appliances

and services, for fast provisioning of unified, optimized networks. They should also enable simple, non-disruptive extension of SD-WAN to on-prem datacenters.

Extending into LANs and WLANs. SD-WAN policy-based management must extend into branch LANs and WLANs to support such common use cases as:

- **Guest Wi-Fi.** SD-WAN solutions must include the capability to define specific policies for performance and security (including web filtering) for guests versus employees to ensure that guests are logged, provided with Wi-Fi, with their content filtered for security, and that their traffic does not impede business performance.

- **BYOD.** Logical segregation of the network into zones allows BYOD traffic or other insecure traffic to be placed on different paths as compared to sensitive/confidential data traffic, in order to help prevent security breaches without requiring significant overhead in management.

- **IoT.** These same required policy capabilities can be extended into IoT environments where IoT traffic should be segregated from traditional traffic for security or performance reasons.

SD-WAN Requirements

The goal is to deploy locally with zero touch via automated activation of all necessary secure WAN gateways, branch LAN switches, Wi-Fi access points, firewalls and WAN optimization; instant extension of your connectivity fabric into cloud networks with one click; and simple, non-disruptive extension of SD-WAN to on-prem datacenters.

To achieve this goal, your SD-WAN must enable:

- ☐ Zero-touch provisioning of new branch equipment without requiring skilled personnel at the branch locations. Establishing connectivity only involves plugging in the power and data cables, which can be done by unskilled personnel at the branch location. Configurations can be made and repeatedly updated from a separate location than the branch, via intuitive workflows that reduce turnaround time.

□ Branch router overlay or replacement with the ability to operate in conjunction with or replace the Customer Premise Equipment (CPE) branch routing device with a "thin" branch device where core SD-WAN and routing capabilities are available on the same physical or virtual appliance.

□ Security via native firewall capability and ability to integrate with third-party CASB or on-prem firewalls.

□ Deployment options with appliances available in physical, virtual, and cloud-based form factors for flexibility to integrate with white box hardware/NFV deployments and into public/private cloud environments.

□ A complete software-defined networking solution spanning all endpoints including secure SD-WAN gateways in the branch, datacenter, and cloud, as well as wireless access points and wired LAN switches in remote business locations.

Summary

As enterprises digitally transform, their networks must provide seamless access to digital services for end-users.

But, with IT more distributed, hybrid, and dynamic than ever, hardware-bound legacy networks can never fulfill this promise. Taming the chaos of IT requires a new approach to networking.

This is the promise of SD-WAN—the ability to use business policies to automate and orchestrate all the components of digital access across a global, unified network.

- **Manage centrally** from a cloud console with a comprehensive view of your enterprise connectivity fabric that connects datacenter and cloud apps with branch and mobile users, all in an integrated management platform that spans and unifies hybrid WANs, cloud networks, and branch wireless and wired LANs with a single policy framework.

- **Orchestrate globally** using business-aligned, policy-based automation to define quality of service and access privileges for all apps and users, combined with automated path steering for hybrid networks, integrated end-to-end performance monitoring, WAN optimization, and security.

- **Deploy remotely with zero touch** via automated activation of all necessary secure WAN gateways, LAN switches, Wi-Fi access points, security services, and firewalls; instant extension of your connectivity fabric into cloud networks with one click; and simple, non-disruptive extension of SD-WAN to on-prem datacenters.

Achieving each of these goals requires both a complete rethink of networking as well as a large number of technical innovations, capabilities, and integrations in order to transform the complex into the simple, the manual into the automated, and the fragmented into a unified whole.

This paper discussed some of the more critical capabilities you need in an effective SD-WAN solution that can carry your organization safely into the digital age. It will benefit your organization to take the time to drill down into the capabilities of potential solutions as well as to kick the tires and test drive before you make the leap. Your business may depend on it.

About Riverbed

Riverbed, at more than $1 billion in annual revenue, is the leader in application performance infrastructure, delivering the most complete platform for the hybrid enterprise to ensure applications perform as expected, data is always available when needed, and performance issues can be proactively detected and resolved before impacting business performance. Riverbed enables hybrid enterprises to transform application performance into a competitive advantage by maximizing employee productivity and leveraging IT to create new forms of operational agility. Riverbed's 28,000+ customers include 97% of the *Fortune* 100 and 98% of the *Forbes* Global 100.

Learn more at riverbed.com