4 Steps to Build an Effective SD WAN Blueprint

By Nitin Mishra
SVP & Chief Product Officer

The concept of Software Define Networking (SDN), while in existence since the 1990s, is attaining greater relevance today. This is mainly due to the growing role of consumer technology, the rise of big data, cloud services and globally distributed networks. In fact, the cloud allows the concept to now be extended to the WAN (Wide Area Network) as well. In fact, enterprises now need to take a critical look at their enterprise WAN Edge, which Gartner describes as the “focus of new architectural approaches”. Gartner further mentions that SD-WAN, Network Function Virtualization (NFV) and alternate delivery models are expected to disrupt the IT ecosystem over the next few years.

Because of the significant value the SD-WAN can provide across, geographically distributed networks, organizations, sooner or later, will need to seriously consider SD-WAN as an essential part of their enterprise architecture. As CIOs start to think about how they need to implement SD-WAN, they need to address a number of issues around connectivity to legacy systems, integration, policies, deployment models, architectural challenges and change management concerns. It is essential for organizations to develop a blueprint that maps individual, functional / departmental, geographical and organizational needs. Here are some of the key steps needed to create a robust, actionable blueprint for SD-WAN implementation.

STEP 1: BALANCE VISION AND EXECUTION

Typical WAN infrastructure is usually a diverse mix of new and old technologies, with different data standards and integration needs. There is no ‘big-bang’ approach to implement SD-WAN technology effectively across the enterprise. Each router, system and controller needs to be replaced or interfaced with SD-WAN technology individually.

The vision of having a single, consistent level of control and agility across the whole enterprise network can only be met through focused, localized and customized execution, which includes:

- Getting complete clarity on your application ecosystem
- Understanding workloads, performance needs and SLA expectations across the enterprise
- Assessing various SD-WAN deployment models (on-premise, hosted, cloud)

So, while CIOs need to build a singular, enterprise vision for their SD-WAN initiatives, they also need to work around current SLAs across various parts of their current networks. This is why, instead of attempting a ‘one-size’ approach, they must align with individual network SLAs at each branch / location.

STEP 2: ADDRESS PERFORMANCE & LATENCY ISSUES

While designing your SD-WAN architecture, you will need to factor different types of workloads at various parts of the enterprise, and their impact on network performance and latency. While supplementing traditional MPLS lines with internet-based links, SD-WAN appliances may often face certain latency issues and local internet infrastructure challenges that need to be streamlined over time. Some of the key considerations while implementing SD-WAN are:

- Selecting private networks or cloud infrastructure: Both options are available for SD-WAN implementations. While private networks have traditionally offered higher performance, more optimized cloud infrastructure and greater bandwidth availability have significantly reduced latency concerns
- Mission critical applications: There may be specialized network components to ensure that mission critical applications always stay within SLAs, in terms of performance, latency and availability.
- Proactive WAN optimization: It is always better to use WAN optimization tools along with SD-WAN appliances, to ensure that performance, latency and response time challenges are addressed.

STEP 3: RELOOK AT YOUR SECURITY NEEDS

With the introduction of SD-WAN appliances (with commodity hardware replacing private MPLS circuits), there are obvious changes to the security ecosystem. On private networks, the need for encryption is much lower as compared to internet based transactions. The greater amount of encryption required to secure SD-WAN based networks puts additional pressure on the network in terms of performance and latency.

The big advantage of using an SD-WAN is the ability to create uniform security policies across the enterprise. This is highly beneficial to organizations which currently have many a patchy security outlay across their branches (usually a combination of MPLS, broadband and other circuits). The ability to deploy security policies quickly and in a uniform fashion allows organizations to set up branch level infrastructure very fast, allowing greater agility and faster response to market needs. A good example is a supply chain management system that provides consistent security policies across its supplier network, by implementing SD-WAN across all their supplier facilities.

STEP 4: BUILD MONITORING & ANALYTICS TOOLS

While deploying your SD-WAN solution make sure you also have the right kind of analytics, visualization capabilities, alerts and notifications to manage network related issues, adjust policies and optimize network traffic flow. Over time, the access to analytics and performance data will enable to network managers to get a stronger understanding of workloads and their unique performance and latency needs. Important features of SD-WAN monitoring include network data analysis, QoS monitoring, Endpoint Monitoring, Component Monitoring and Access Management.

SD-WAN is much more than an emerging trend in the networking space, and promises significant value to organizations as they grow and evolve in an uncertain business environment. An effective SD-WAN implementation strategy would involve a combination of cloud-based appliances and managed services. Managed service providers like Netmagic actually have an entire suite of SD-WAN offerings with robust SLAs, allowing customers to combine state-of-the-art cloud infrastructure with an extensive suite of cloud (storage, network and compute) services.