Enterprise Digital Transformation with SD-WAN and 5G

Naresh Thukkani
VP of Products ,Criterion Networks

Digital transformation is the need of the hour for almost all enterprises globally. Many companies are embracing the mobile, video, cloud and IoT technologies in order to stay competitive and relevant with the ever-growing demands from their customers and partners. Most CEOs, CTOs and CIOs agree that the risk of going out of the business is definitely high without incorporating digital strategies in their portfolios. Accordingly, we see a good amount of investment in the budget going towards the research, deployment of new digital methodologies and upskill of their workforce in this direction.

Enterprises are now planning to implement multiple new services as part of the digital transformation strategy across their LAN, WAN, and DC. In this paper, we will mainly focus on the requirements like Multi-Cloud, Bandwidth hungry Apps, Security, IoT & Edge Computing requirements and the challenges that need to be resolved on the WAN segment in particular. There are a good amount of developments happening in the enterprise LAN and DC space and we will focus on them in another paper.

Multi-Cloud

Today, given the economics of cloud computing, it is a no brainer today for most CIOs to comfortably move their workloads on cloud providers like AWS, Azure and GCP and leverage other SaaS applications. While few enterprises are going with a single cloud provider, the majority of the enterprises are embracing multiple cloud providers to avoid vendor lock-in. Apart from vendor lock-in, it is becoming more evident that few workloads seem to perform well or integrated better with an ecosystem of tools in one provider cloud compared to others. Hence, in order to get the best of breed services for a wide variety of application requirements, enterprises are looking to have their workloads spread across multiple clouds. It is worth to be noted that many of these cloud services might have their own application SLA requirements to perform better.

Enterprises typically used the Datacentre as the central wall of defence where they hosted many security appliances to inspect the traffic that was going in and out of the organization. While the architecture worked well so far, this approach may not work for the multi-cloud strategy many enterprises are planning to implement. Cloud applications that reside on the Internet need to get the best SLAs to ensure a great experience for the employees. Backhauling all the traffic for cloud applications from branches to data centers and from there to the Internet increases the latency and accordingly a poor experience.

For example, an enterprise with 70K employees who plan to move their email application server from in-house to Office 365 need to carefully think of the dependencies on the network characteristics so that the O365 application to perform better without compromising the quality and poor user experience for their employees

Bandwidth Hungry Apps

In an enterprise, the demand for the WAN bandwidth is clearly very high nowadays. This can be attributed to the growing number of a wide variety of bandwidth-hungry applications and end-points used by the employees, partners, and customers. In order to ensure an overall quality experience, the underlying BW has

to increase so that the applications are not starving. While the enterprises typically used MPLS as the primary way of communication across the network for all applications, procuring more MPLS bandwidth for growing bandwidth needs is not a long-term scalable cost-effective solution. Hence, enterprises are looking to have other alternative links like low-cost Broadband Internet as the primary vehicle for communication along with MPLS.

However, given the best effort and less secure behaviour associated with broadband Internet & 4G, IT teams are facing challenges in setting up needed secure tunnels, managing the application traffic into respective tunnels and ongoing changes to the deployment. Additionally, the complexity increases as well with the ever-changing IT policy decisions by the management as per new business interests. Hence, there is a need for efficient WAN management to support applications with less operational complexity to ensure IT teams are adding significant value to the business.

Security

While the enterprises are marching towards the digital transformation journey, many elements need to be addressed in the right way to ensure they are still compliant with the auditing and regulatory standards. Given that the data has to be secured before, during and after the transaction has happened, security has to be treated as a high priority and look out for solutions from vendors who help them in accordance with their principles.

If an enterprise that moved the documents to an AWS cloud and an engineer incidentally opens the S3 document permissions as public or allowed complete access to an important application, it can be a serious situation for the company and brand recognition. The complexity manifests even more if the enterprises have multiple cloud providers in place and the engineers need to be trained and certified on multiple domains. Hence, the right skill set, monitoring and visibility tools, network and security policies should be in place to avoid any breach of security.

IoT and Edge Computing

Many IoT end-points like electrical/mechanical/medical sensors, video surveillance cameras etc are being deployed in enterprises to support various use-cases. It is expected that 5.8 billion IoT devices will be deployed overall by 2020 in enterprise and automotive markets. Given the huge deployments of IoT devices in the enterprise, it is nearly impossible for IT teams to manage them manually and hence there is a need for automation, analytics, and assurance of policies that govern the IoT deployment in an agile manner. Additionally, in specific IoT deployments, it is also not possible for IoT devices to send all the data remotely to a cloud or data centre which are many miles away to take critical decisions to turn-off or turn-on certain devices. Hence, enterprises are exploring the option of edge computing to collect the IoT data, process, store and take the decisions locally and periodically transfer the data to remote centres for backup of data. In order to help with better local decision processes at the IoT edge, machine learning/artificial intelligence algorithms can be used at the remote data centre and the resultant schema can be pushed periodically to the IoT edges across the enterprise.

SD-WAN at the rescue for Enterprises

SD-WAN is the new framework that is widely used to solve these challenges along with many other business-critical challenges. SD-WAN abstracts the underlying transport links/characteristics at every branch and views them as a single logical link for management purposes. It automatically sets up the secured tunnels in a zero-touch fashion and dynamically adjusts the paths based on network conditions. This completely eliminates the need for manual setup of tunnels. SD-WAN operators can define the traffic policies along with pre-defined conditions or SLAs for the entire network at a centralized location. This greatly simplifies the operational complexity and based on the

policies defined, traffic moves accordingly on any of the underlying transport links that satisfies the pre-defined conditions. Operators can additionally fine-tune policies at every branch as needed to accommodate any local conditions or needs. SD-WAN provides the freedom of choice for enterprise operators to now choose any underlying transport from a wide variety of choices without worrying about the complexity associated with them.

Since the Internet-based SaaS/Cloud applications prefer lower latencies, traffic can now be directed to the Internet from the branch directly without backhauling the traffic to a DC and exiting from there. This will greatly improve the user experience as needed for Multi-Cloud applications. Another important aspect to achieve this is the Deep Packet Inspection (DPI) capability on the SD-WAN edges where most of the applications for the enterprise can be detected and the right treatment can be provided to them as defined by the policy. Since we are now exposing the branch directly to the Internet, one might wonder about the security implications and compliance/regulatory considerations in such implementation.

SD-WAN Security offers a set of choices to secure the network completely. Today, we see many Internet cloud security solutions like Cisco Umbrella, Zscaler etc being available and enterprises can centrally define to redirect the traffic to these security cloud providers from their branches before reaching Internet SaaS/Cloud applications. More importantly, the SD-WAN routers at the branches are being enhanced to support security capabilities like Zone-Based FW, IDS/IPS, URL-Filtering, Advanced Malware Protection. Together with these inbuilt security features, connectors to Cloud security and Service Function Chaining capabilities to insert any other security appliances along the traffic path, SD-WAN has great things to offer to the end-customers.

5G is a Game Changer

As mentioned earlier, SD-WAN abstracts the underlying transport links like MPLS, broadband Internet, 4G and decreases the complexity for operators without worrying about the internal implementations. From that perspective, 5G can be thought of as just another new form of communication that provides high bandwidth to an enterprise and SD-WAN manages the traffic across all the available links (MPLS, Broadband, and 5G) in an efficient way as per network conditions. However, given the capabilities of 5G technology like greater throughputs, lower latencies, enhanced security, ultra-reliability, and energy efficient networks for businesses, SD-WAN policies can be fine-tuned to achieve the best possible output for specific use-cases and next-generation enterprise applications.

What is 5G and how does it help?

5G is the new generation of cellular technology that has the promise to offer greater throughputs, lower latencies, enhanced security, ultra-reliability and energy efficient networks for businesses, end-users and IoT end-points. In order to achieve the 5G goals, both the end devices and the telecom operator infrastructure have to transform in a big way. The key aspects like MIMO (Multiple-In Multiple-Out), high-frequency waves, beamforming, small cell deployments are needed from the transmission edge devices/air-interface perspective and more importantly, the complete virtualization of the current telecom physical infrastructure (compute, network and storage) using SDN/NFV is needed to achieve the 5G goals.

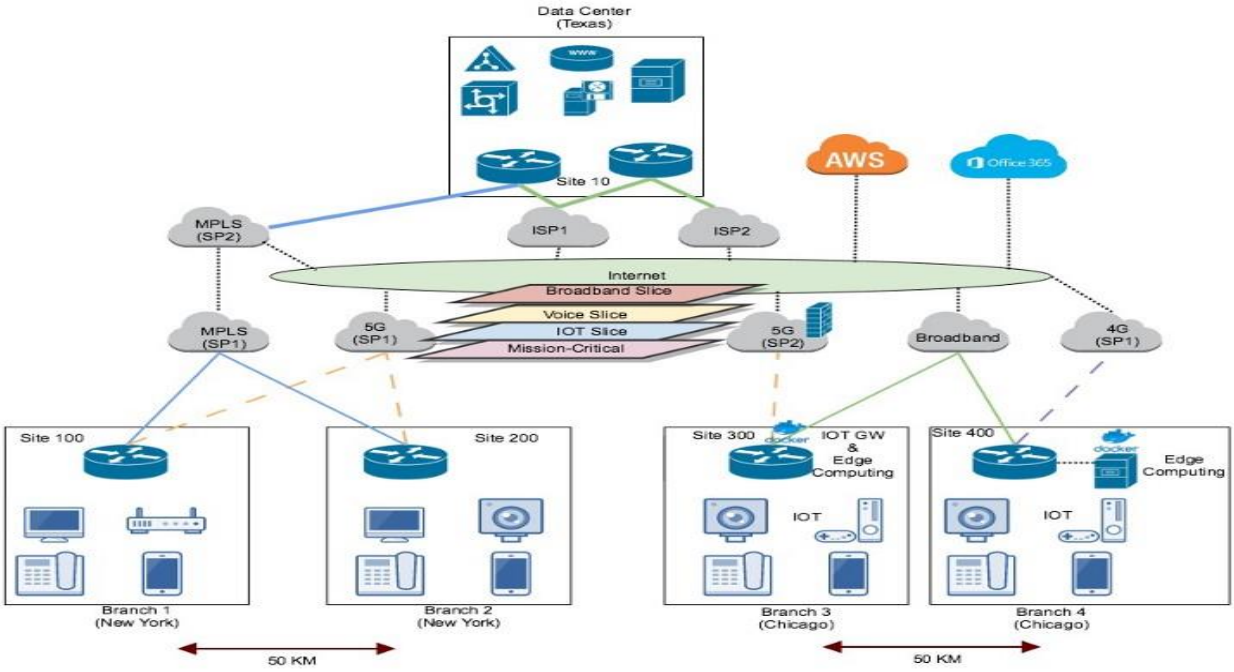
Given the promising 5G performance attributes, it has the potential to address many use-cases ranging from mission-critical applications that require extremely low latency to big data/VR/AR applications that need higher bandwidth. Service Providers are investing a lot in 5G transformations to reap the benefits in front of them by serving the enterprises, end-users, IoT devices, and their applications. Enterprises are looking to leverage this

opportunity to augment their existing services with the next-generation applications to stay competitive and relevant to their customers and partners. Retail end-users are looking to have better connection speeds to enable them with a great video quality experience, downloads of large files at the click of a button, immerse in a brand new AR/VR applications while on the move. Home users can also leverage a 5G wireless router that is not tied to the fixed location and property and carry as they move. IoT devices are expected to reach 20 billion by 2022, it is very important for them to stay connected at every moment to transfer the mission-critical, higher bandwidth data to other locations for processing, analysis and storage and 5G is seen the reliable technology to make the IoT deployments successful.

5G Network Slicing

Service Providers are transforming their existing physical infrastructure to support virtualization using SDN/NFV from the past 3–4 years. Network Slicing is an important outcome of this transformation that has the potential to change the way networks are going to be consumed in the future for the enterprises. Network Slicing is the ability for an enterprise to subscribe for a slice (compute, network and storage) of operator infrastructure for a part-time or full-time commitment. During the subscription, the enterprise can specify the performance attributes they are interested in to support their use-case. For example, to support the mission-critical medical applications, they can request for a slice that provides ultra-low latency at 1ms. For some enterprises, IoT could be a major application that demands bandwidth of 1 Gbps and 10ms latency. Service provider than bring up the needed elements in the virtualized infrastructure to support the SLA requested and assigns to the respective customer. This greatly increases the security between multiple customers. This is also significantly different from previous 4G implementations where the SLA guaranteed is across all compute, network and storage domains. It is also possible for a single end-point to subscribe to multiple network slices. This supports many use-cases for enterprises where they can use the first low latency slice for the gathering critical data and use another slice for reporting only the critical data after processing.

Please have a closer look at the below figure that highlights the typical enterprise deployment with key elements



· Multiple Service Providers (MPLS, Broadband, 4G, 5G)
· 5G Network Slices (Broadband, IoT, Voice, Mission-Critical)
· Site 10 is Data Centre (Texas) that hosts various enterprise apps
· Site 100 is the New York branch with voice, data, mobile, wired and wireless devices
· Site 200 is another New York branch within 50 KM distance to Site 100
· Site 300 is Chicago branch that has voice, mobile, IoT end-points like Video game console, Video surveillance cameras
· Site 400 is another Chicago branch within 50 KM distance to Site 300
· Site 300 SD-WAN router is also an IoT Gateway and Edge Computing node
· Site 400 SD-WAN router is connected to another server for Edge Computing
· 5G SP2 (Chicago area) also provides VNFaaS with Firewall functionality
· Employees are accessing AWS, Office365 applications across the Internet along with other enterprise apps in DC

5G Broadband Slice

This is the first use-case where 5G serves as a normal broadband Internet connection. Enterprises can subscribe to a network slice with BW requirements and telecom providers can provide the required BW. As discussed earlier, SD-WAN helps in simplifying the operational complexity of provisioning and managing the WAN network for this enterprise. From the 5G perspective, Site 100/200/300 routers have subscribed to "5G Broadband slice" along with other transport links. Based on the centralized SD-WAN policies or primary paths defined by the operator, traffic will be moved among any of the transport links by taking into consideration of the underlying transport link network conditions. In case of any change in network conditions, traffic dynamically shifts to other transport links assuming they meet the SLA considerations of the applications.

5G Voice Slice

In the second case, enterprise Site 100 and 200 have also subscribed for a "5G Voice Slice" from the same SP. Since voice is very critical for their operations, they have planned to get a better latency SLA compared to Broadband slice. Now, if you are wondering about how the traffic will be sent across the voice slice only for voice traffic, SD-WAN has an elegant solution for it. SD-WAN routers have the ability to match on certain application traffic defined by the operator and can seamlessly route traffic into the respective slice. In this case, any voice traffic can be sent to Voice slice and other regular traffic can be sent to 5G Broadband slice. In case of any issues with the voice slice temporarily, SD-WAN has the inbuilt robust mechanism to redirect the voice sessions to other transports in the order of priority based on the policies defined.

Without SD-WAN, it would be a nightmare for the IT teams to define the configurations manually and push to multiple sites in real-time. Assuming, the enterprise needs to allow another important traffic like a voice on to the same "5G voice slice", they can simply update the centralized SD-WAN policy to accommodate it at the click of a button.

5G IoT Slice—Edge Computing and SD-WAN

In the third case, IoT devices at the sites 300 and 400 need to send critical data and wait for the action to be taken by them after the data is analysed. Enterprise Site 300 router is also subscribed for "5G IoT slice" Site 300 router is also an IoT GW, all the IoT devices in both sites 300 and 400 are using this slice to share the IoT data with the IoT GW router. In this case, IoT 5G slice can help extend the traditional physical boundaries of the site 300 by incorporating the IoT devices in site 400 or in other sites

as long as they are in the vicinity of the application SLA needs.

While the IoT GW received the data using “5G IoT Slice”, Site 300 router also the Edge computing node capabilities with Docker integration. Since the action to be taken is critical, it works best to process the data locally than sending the complete data to the remote cloud site. It greatly increases the efficiency of the IoT deployments using edge-computing techniques. However, for auditing, monitoring and analytics purposes, data can be sent back to remote cloud sites as a backup. In order to send the backup data, Site 300 router might use any of the transport links like “5G Broadband slice” or MPLS. Additionally, given the advancements in Machine Learning (ML) and Artificial Intelligence (AI), received large data sets at the remote site can be used for processing and training the Machine learning models and the resultant schema can then be sent to edge computing branches to facilitate better decisions locally as the deployments mature.

In some cases where the processing load is heavy on a site 300, the router might also redirect the traffic to the site 400 to leverage the dedicated edge-computing node processing power. Such a traffic redirection is possible with SD-WAN in a simple and effective way

5G VNFaaS

From a security perspective, it is possible for the enterprises to also leverage the security FW provided by the telecom provider along with the SD-WAN security at the edge. Enterprises can request for a network slice with VNF service along with other performance attributes discussed above. In this case, FW can be inserted into the “5G Broadband slice” during the subscription and all the traffic from the branches will be sent to the FW for inspection and reaches to the Internet if the traffic is allowed. Enterprise operators can still control FW policies to suit enterprise requirements. Such use-cases are very exciting for the telecom service providers where they can now monetize the enterprise requirements by providing value-added services.

Summary

Enterprises globally are undergoing a major digital transformation to include multi-cloud services, high bandwidth applications, Security, IoT devices and Edge-computing nodes. SD-WAN greatly helps the enterprises to make the network application-aware and route the traffic as per the predefined policies and network conditions. Its centralized management will help the IT teams to reduce their operational complexity and focus on providing the best value to the business. Enterprises can greatly benefit from 5G technologies in combination with SD-WAN to accommodate next-generation mission-critical applications of the enterprises and seamlessly manage the large-scale IoT deployments along with Edge computing capabilities.