Software defined networking (SDN) for campus networks, WAN, and datacenter

DAVID, Olubukola, THORNLEY, Paul and BAGHERI, Maryam

Software Defined Networking (SDN) for Campus Networks, WAN, and Datacenter

Olubukola David
Sheffield Hallam University
United Kingdom
Bukkyokunwobi@gmail.com

Paul Thornley
Sheffield Hallam University
United Kingdom
P.Thornley@shu.ac.uk

Maryam Bagheri
Sheffield Hallam University
United Kingdom
Maryam.Bagheri@shu.ac.uk

***Abstract*- As the demand for internet and cloud services continues to grow, enterprise network infrastructures are becoming complex to manage. Methods of deployment and management of traditional network devices can become cumbersome and error prone as infrastructure complexity increases. Thus, the need for an easier but highly effective and secured networking approach to confront the growing demands of network environments is necessary. In recent years, software defined networking (SDN) became an effective way that supports the future of networking especially with the introduction of virtualization and cloud computing. The adoption of SDN concepts across different organizations, offers advantages resulting in the reduction of operational cost using simplified software, hardware, and management method. This paper reviews some of the current SDN solutions developed for campus networks, wide area networks (WANs) and datacenters identified by the Gartner Peer Insights reviews. A survey was also conducted to find out how these solutions have been adapted in different organizations.**

Keywords- Software Defined Networking (SDN), Campus Network, WAN, Datacenters

I. INTRODUCTION

With the introduction of new technologies such as cloud computing and virtualization, the demand for interconnectivity continues to grow rapidly, creating the need for more innovative way to tackle the issues that confront traditional networking [1]. For instance, in traditional networking, devices like firewall, routers and switches which are manually configured would need to be reconfigured and updated when there are new services available. This is quite complicated especially in large networks. With some of these obvious and continuous challenges, the need for a more dynamic networking approach that unifies network management and provisioning becames more evident [2]. Over the past few years, SDN has become an efficient approach that provides a more and scalable solution for network management and configuration. Studies carried out in previous years formed a part of the current development and adoption of SDN. An example is the Stanford University Clean Slate project done in United States in 2006 among several others [1]. The concept of SDN came alive with the desire to have a flexible and centralized management of forwarding in network devices [2]. Therefore, SDN gives the ability to manage networks dynamically, by having the control and management plane decoupled from the data plane while the network becomes programmable using a centralized controller, thus, influencing the overall network performance [3].
According to [3], various SDN solutions from different vendors were designed to address, high availability, scalability, and reliability issues in the traditional networks. Many companies have already adopted SDN to manage and enhance the control over their networks and it has been predicted that the SDN market value as of 2020 is $8 billion and it is estimated to be worth over $43 billion globally by 2027 [4]. In this paper we review the current trends in SDN for different areas of networking including campus networks, WANs, and data centers. This will provide an insight into the benefits and some of the current challenges that still exist while deploying these SDN solutions. Furthermore, this paper could provide guidance and considerations for network specialists and key stakeholders when selecting specific SDN vendors for deployment within their infrastructures. The rest of this paper is structured as follow; section two presents a review of the current SDN solutions for different areas of networking. In section 3, the research methodology, data collection and data analytics will be discussed in detail followed by discussion and conclusion.

II. SOFTWARE DEFINED NETWORKING (SDN)

The emergence of software defined networking is rapidly changing how organizations approach network management and operation. This moves towards a fluid and dynamic network which automates response to organizational demand and introduces financial benefits through reduced OPEX and CAPEX costs [5]. To achieve these financial benefits, SDN architecture incorporates several cloud computing attributes such as scalability, elasticity, availability, resiliency, and redundancy that are required for successful deployment of SDN solution [6] [7]. The operational benefits of introducing SDN based technologies within a networked infrastructure has been widely discussed in the literature. Several studies suggest that the implementation of SDN technologies provides significant improvements in network scalability, elasticity, network management, and response to demand in comparison to using traditional networking hardware and concepts [8][9]. In this

979-8-3503-0252-3/23/$31.00 ©2023 Crown

section we introduce different SDN based solutions developed by different vendors for Campus networks, WANs, and datacenters.

A. Campus Networks SDN Solutions

1) Cisco Software Defined Access (SD-Access)

Cisco provides the Cisco SD-Access framework as a GUI-based platform for configuring and deploying Cisco DNA Center (C-DNAC) within campus networks. This is split into two key areas: Cisco DNAC providing the management and automation; with Cisco Campus Fabric providing the underpinning infrastructure within a Cisco SD-Access campus network [10]. The Campus Fabric is used to provide the control, data, and policy plane of networking and applies the underlay and overlay fabric technologies within its SDN architecture. Both fabrics operate independently from each other with the overlay fabric providing the separation of the control plane logic away from the overlay fabric networking devices with similar occurring within the underlay fabric. According to [11], the process of the underlay fabric deployment can be automated through the Cisco DNAC solution. Deploying the underlay/overlay fabric networks with automated fabric development could introduce significant flexibility, scalability, and programming opportunities within SDN infrastructures

2) Cisco Network Service Orchestrator (NSO)

Services and infrastructure implementation within organizations is becoming progressively complex, often incorporating hybrid systems with physical and virtual systems operating in coexistence with each other. To add more complexity, the operation of these systems often falls into specific domains such as Access, WAN connectivity and datacenter; resulting in the need to use management systems and methodologies for deployment of services within these domains. Cisco NSO provides an abstraction layer between the north-side services such as scripts, applications, DevOps, CI/CD pipelines; and the complex muti-domain systems on the south-side such as multi-vendor networking hardware, containers, and virtual machines [12][13]. Cisco NSO uses the YAML data model, a centralized Configuration Datastore (CDB) and Network Element Drivers (NEDs) to provide the full abstraction of configuration and management. Interaction with the CDB operates similarly to traditional database transactions where all changes to the infrastructure are all applied at once in one transaction, with any failures rolling back to the stored configurations within the CDB. The NEDs facilitate changes stored to the CDB or actioned within the YAML file to the required infrastructure nodes. Using YAML provides a standardized format for making changes and eliminates errors and labor-intensive tasks inherited through traditional CLI management and configuration [12].

3) Juniper SDN (Contrail Networking)

Contrail is an SDN solution providing networking within cloud and virtualized networking infrastructure operating within an overlay fabric. Contrail integrates with systems such as OpenStack and CloudStack as an Infrastructure-as-a-Service (IaaS) to provide automation and orchestration of virtual systems such as virtual networks (VMs) and virtual routers. Contrail is split into two components: the Contrail SDN controller providing the northbound and southbound abstraction; and vRouters providing the forwarding plane operating within the hypervisor of a virtualized system. vRouters establish logical tunnels (overlay fabric) between each other using physical networking devices within the underlay fabric. Juniper Contrail use either MPLS over GRE/UDP or VxLAN tunnels to facilitate the separation of traffic and multi-tenant environments [14]. The northbound interface within Juniper Contrail is achieved using REST APIs and provides the capability to integrate with the Contrail GUI or other orchestration applications. The southbound controller uses Extensible Messaging and Presence Protocol (XMPP) to communicate network changes to vRouters; with BGP and NETCONF providing the southbound interface to physical network hardware. Additionally, the Contrail SDN controller provides East-to-West interfaces using the Border Gateway Protocol, allowing peer-to-peer controller communication [14].

B. WAN SDN Solutions

1) Cisco SD-WAN (Cisco Viptela)

In 2017, Cisco completed the acquisition of Viptela, a SD-WAN based solution and introduces the concepts of Software Defined Networking into WAN connectivity within complex enterprise networks. The Cisco SD-WAN solution uses a vSmart controller to facilitate communication between each vEdge Router situated on the edge of enterprise campus networks. The vSmart controller uses the Overlay Management Protocol (OMP) over a DTLS/TLS connection within the southbound interface, providing the abstraction of the management/control planes typically found within SDN solutions over WAN connectivity [15]. By introducing SDN concepts into WAN connectivity provides scope for controlling routing and traffic shaping decisions based on programmability, automation, and application layer (Layer 7) services. Within Cisco SD-WAN, network management and data gathering operations are achieved by using vManage presenting the vSmart controller with a northbound interface. This facilitates the delivery of CRUD actions to the vSmart controller using either the vManage REST API, Netconf, direct CLI commands or SNMP. Data gathered from vEdge routers is stored within the vManage statistical database and can be presented to the user via the vManage user interface. Furthermore, the use of REST APIs provides scope to utilize non-proprietary or bespoke software to interact with the vSmart controller [16]. However, complex enterprise-to-enterprise WAN connections are challenging to deploy as the number of enterprise edge devices expands. To address this issue, Cisco SD-WAN introduces vBond to provide mechanisms to provision and deploy new networking nodes. The vBond orchestrator initializes the process of authenticating and authorizing new node deployment within the SD-WAN network and provides a template for device configuration [17].

2) Cisco Meraki

Cisco Meraki provides a cloud-based management platform which can be utilized to manage enterprise WLAN, LAN and SD-WAN solutions for branch-to-branch connections through its Meraki edge devices [18]. All deployment, orchestration and management activities are conducted through the Meraki dashboard which is a centralized cloud-based application accessible over the public internet. Whilst the Cisco Meraki SD-WAN solution does not operate a on-premises controller found within typical SDN architecture, this solution provides cloud-managed automation within WAN environments and can apply Policy Based Routing (PBR) and Dynamic Path Selection (DPS) on a per path basis using 'AutoVPNs'. This allows for the selection of specific paths and VPNs based on network performance, application type and load balancing [19]. AutoVPN operates using a server-client model and situates a VPN registry within the Meraki Cloud service and contains the VPN attributes required to form secure tunnels [19].

3) Fortinet Secure SD-WAN solution

Common tasks within traditional firewall operations are becoming more commonly integrated with other infrastructure security mechanisms such as Deep Packet Inspection (DPI), Intrusion Prevention Systems (IPS) and Web/Application Filtering to form Next-Generation Firewalls (NGF) [20]. According to [21], the FortiGate family of NGFs, can be deployed as a physical, virtual or hybrid NFG appliance. Where Fortinet Secure SD-WAN solution differs from other SD-WAN solutions is the integration of SD-WAN processes with infrastructure security mechanisms often found within NGFs. Fortinet break down its secure SD-WAN solution into 4 high level components: FortiGate (Appliance/Hardware), FortiOS (Operating System), Fabric Management Center (Centralization/Orchestration) and FortiGuard (Threat Reporting/Detection/Prevention). Whist the Fabric Management Center provides a centralized interface for the provisioning and configuration of Fortigate Appliances, each device can be accessed via REST APIs allowing the creation of automation scripts using Python, Ansible and Terraform.

4) Palo Alto Prisma SD-WAN Solution

This solution compromises of a cloud-based centralized controller and provides the abstraction of the control and management planes typical of SDN architecture. The data plane remains on the Palo Alto ION (Instant-On Network) nodes forms VPN tunnels with other ION nodes in accordance with the policies configured on the controller. Secure connectivity between the ION nodes and the Prisma controller is achieved using Transport Layer Security on port 443 (HTTPS) [22]. Once an organization acquires and installs an ION device, the node contacts the controller over a typical TLS 1.2 session and authenticates using a pre-installed Manufacturer Installed Certificate (MIC). Administrators can then 'claim' the device within the Prisma controller where a Customer Installed Certificate (CIC) and a unique device ID is created and pushed to the device over a TLS 1.2 session. To partake in network activities and form VPN tunnels with other ION nodes, polices are attached to ION devices including any node specific configurations. Once the attributes have been configured, they are then pushed to the ION device and can participate in typical networking tasks and form VPN tunnels with other ION nodes.

C. Data centre SDNs

1) Cisco Application Centric Infrastructure (ACI)

Cisco ACI solution primarily focuses on providing SDN capabilities within the datacenter spine and leaf topology. Abstraction of the data plane, typically found within SDN architecture, is achieved by the installation of the Cisco Fabric Operating System within the Nexus 9000 series of switches. The Cisco Application Policy Infrastructure Controller, managed within Cisco Nexus Platform is used to deliver Layer 3 switching policies, routing and other traffic management configuration to the Nexus 9000 series fabric switches [12]. To allow management of both physical, hybrid and multi-cloud environments, Cisco ACI also supports integration with Open vSwitches (OVS), VMware, Hyper-V and Kubernetes products to operate in conjunction with physical Nexus 9000 switches. Through this integration of cloud environments, administrators can control, manage, and deliver network policies and changes to multi-environment devices through the Cisco APIC. Furthermore, Cisco ACI allows integration with Cisco Viptela SD-WAN to provide the best route from end user within branch, to the application running within the Cisco ACI managed datacenter [12].

2) VMware NSX

In a similar approach to virtual machines, VMware NSX provisions virtual network infrastructure in response to network and application demands that can extend over multiple datacenters operating within private, hybrid and public cloud, or across multiple containerized environment [23]. VMware NSX operates an underlay/overlay architecture by removing dependence between the layer 2/3 logical networks within the overlay, from the physical hardware within the underlay network. VMware NSX provides a REST API, allowing cloud management platforms to fully automate the creation and deletion of logical overlay networks. The control plane operates within the VMware NSX Controller cluster and is responsible for managing routing and switching within the hypervisor with the data plane remaining on the virtual appliances. To provide resilience and high availability, NSX controllers are clustered and managed by NSX Manager must contain at least three nodes. An inherent risk of clustering is the introduction of a 'split-brain' scenario where two controllers have become separated due to failure and are now both independently sending control plane messages with nodes within the NSX Domain. To prevent this, each Controller cluster must operate within a Quorum where the majority of NSX controllers within the domain, are used to disperse control plane messages within the NSX Domain.

3) Juniper Apstra

Juniper Apstra is a solution that provides a single platform for the provisioning, management, monitoring and troubleshooting devices deployed within the datacenter. For commonly performed tasks and deployment attributes, blueprints can be created within Juniper Apstra. These blueprints are used to compare and test network nodes during deployment and orchestration against the template attributes. The Juniper Apstra controller provides the abstraction of the control and management plane from the datacenter fabric and allows for Intent-based Networking (IBN). IBN is the removal of individual configuration tasks and actions required for the network to fulfil business requirements. Networking administrators within an IBN environment only need to address the overall outcome of the network. The Juniper Apstra solution completes all tasks, verifies configurations against blueprints, and makes dynamic adaptations to networking devices to achieve the overall business goal using machine learning and Artificial Intelligence.

D. Open-source SDNs

1) OpenDayLight SDN Controller

In 2013, the Open Network Foundation in partnership with the Linux Foundation created the OpenDayLight (ODL) SDN Controller. The motivational factor for the development of ODL was the prevalence of issues within previously released SDN controllers. As a result, a new SDN controller was established and involved the collaboration of multiple vendors creating a more efficient and stable SDN controller. This has made ODL one of the most utilized open-source SDN controllers and has had a significant influence on commercially available SDN solutions [24]. To deploy, installation of ODL controller is required on a Linux-based system within a Java Runtime Environment (JVE) and can be presented to a network as either a virtual machine or on physical hardware. Once ODL controller is operational, Apache Karaf is used to install specific feature bundles allowing administrators to deploy feature sets that is fully tailored to the organizational needs of the network infrastructure [24]. OpenDayLight can be used as a viable and deployable solutions within small to medium-sized business networks [35].

2) Floodlight SDN Controller

The Floodlight SDN controller operates and draws similar functionalities to the OpenDayLight controller, with the northbound API providing application interaction through a REST API. The southbound controller utilizes the OpenFlow protocol and provides interaction between networking devices and creates the abstraction as discussed in [25]. As a result of the similarities, the method of deployment is very similar to the OpenDayLight controller and can be deployed within a Linux OS or as a stand-alone virtual machine. The floodlight controller supports Open vSwitch for virtualized switching technologies [26].

3) Open Network Operating System (ONOS)

Similar to the OpenDayLight and Floodlight SDN controllers, Open Network Operating System (ONOS) can be run on Linux machines or as a stand-alone virtual machine and was developed by the Open Network Foundation (ONF). In comparison to traditional network management systems, the ONOS controller requires minimal hardware requirements [27] and could be deployed on large servers, down to small devices such as a Raspberry Pi.

III. Research Methodology

As the literature shows there are a multitude of studies conducted discussing different aspects of SDNs including architecture [28][29], implementation [2], security [32] and performance issue in SDN [34]. In this research, we analyze market leading SDN based solutions introduced in the previous section to identify key features and drawbacks for utilization with enterprise networks. To do so a qualitative research approach has been conducted and two sources of data has been used, data from Gartner Peer Insights [30] and to gather a broader and in-depth knowledge of how SDN has been used in organizations, a survey was also conducted. The survey was distributed among IT professionals especially network administrators, network engineers, and SDN experts.

A. Data Collection and Analysis

1) Gartner Peer Insights Reviews on SDN

The data gathered from the peer reviews are based on user experience extracted from Gartner Peer Insights [30], copy right 2022. The reviews were verified, and the participants involved were various organizations that have had first-hand experience with the reviewed products. The review contains data gathered within the survey spanning from 2018 to 2022. Relevant information about some SDN solutions were gathered in 3 categories: WAN, Datacenter, and the campus network. Information about deployment region were captured, company size, industry, and customer experience were also collected. The size of the organizations utilizing SDN solutions were categorized in terms of revenue. Thus, organizations with revenue of < 50M USD were categorizes in this article as small enterprise, while organizations with revenue of 1B to 10B USD were categorized as medium sized enterprise and organizations with above 10B USD were categorized as large enterprise. Other key areas mentioned by the reviewers such as, cost and drawbacks were also extracted.

a) Gartner Peer Review on some SDNs for campus network

Table I shows data gathered within the review for the deployment of SDN solutions within campus networks. Based on the collected data from 20 reviews, Cisco NSO is a solution that can be used in all small, medium, and large organizations. Juniper SDN is mostly used in medium and large organization. No information was found on Gartner Peer Insights website about Cisco SD-access.

TABLE I. SDN SOLUTIONS FOR CAMPUS NETWORK - GARTNER PEER INSIGHTS REVIEWS

Solution	Company size	Features	Cost	Drawbacks
Cisco NSO 3 reviews	Large Enterprise (33%) Medium Enterprise (33%) Small Enterprise (33%)	-Automation -Multi-vendor capability -Ease of service modellin -Faster and easier integration of new services	N/A	N/A
Juniper SDN (Contrail Networking) 17 reviews	Large Enterprise (47%) Medium Enterprise (41%) Small Enterprise (N/A) Government Enterprise (12%)	-Simple user interface -Automated Integration, interoperability -Very good L3 functionalities -Good performance -Support major platforms on hypervisors	Reasonable Price	-Difficult to deploy -Very low documentation -Steep learning curve
Cisco SD-Access	N/A	N/A	N/A	N/A
(317 reviews)	Small Enterprise (13%) Government Enterprise (7%)	-Improves performance -Easy to configure and monitor		Fortigate or Fortimanager
PALO ALTO Prisma SD-WAN (306 reviews)	Large Enterprise (51%) Medium Enterprise (39%) Small Enterprise (8%) Government Enterprise (2%)	-Automation, Security -Easy to deploy, use and operate -Ease of integration -Scalable -Good GUI interface -Zero touch provisioning	Quite Pricy	Product licensing is expensive Sometimes slow management interface
Cisco Viptela SD-WAN (69 reviews)	Large Enterprise (46%) Medium Enterprise (41%) Small Enterprise (7%) Government Enterprise (6%)	-Automation & Central management -Security -Easy User Interface -Fast configuration and deployment -Good support team	Flexible Pricing based on need Lower cost compared to MPLS	Licensing is complicated to understand and can get expensive Prize is high for use cases of small extensions such as small branches
Cisco Meraki SD-WAN (116 reviews)	Large Enterprise (40%) Medium Enterprise (47%) Small Enterprise (9%) Government Enterprise (3%)	-Automation & Central Management -Security -Cloud Based -Fast Deployment and -Ease of Use	Reduced cost compared to MPLS	Tedious and time-consuming Initial implementation .

b) Gartner Peer Review on some SDNs for WAN

Table II highlights a comparison between some WAN SDN solutions. In total, there was 317 reviews for Fortinet SDWAN, 306 reviews for Palo Alto Networks, and 116 reviews for Cisco Meraki and 69 reviews for Cisco Viptela. In the Gartner peer review, even though the number of professionals that reviewed each SDN solution for WAN varied in size and demography, result shows that only a few percent of reviews are from those IT professionals who work in small enterprises. For example, with Cisco Viptela, only 7%, PALO ALTO Prisma 8%, Cisco Meraki SD-WAN 9% and Fortinet FortiGate Secure SD WAN 13% of reviews are from experts in small networks. Likewise, for medium sized Enterprise, Cisco Viptela SD-WAN 41%, Cisco Meraki SD-WAN 47%, Fortinet FortiGate Secure SD-WAN 60%, and PALO ALTO Prisma SD-WAN 39% reviews are from people working in medium sized Enterprise. With Cisco Viptela SD-WAN 46%, Cisco Meraki SD-WAN 40%, Fortinet FortiGate Secure SD-WAN 20%, and PALO ALTO Prisma SD-WAN 51% reviews obtained from professionals in large enterprises. Evidence shows that even though small enterprises are beginning to adopt SDN solutions for their WAN connectivity, over 80% of the respondents using SDN in their WAN were from large and medium sized enterprises.

TABLE II. SDN SOLUTIONS FOR WAN - GARTNER PEER INSIGHTS REVIEWS

Solution	Company size	Features	Cost	Drawbacks
Fortinet FortiGate Secure SD-WAN	Large Enterprise (20%) Medium Enterprise (60%)	-Automation -Security -Easy to deploy, integrate, and control	Cost Effective	Some functions require CLI commands and cannot be completed via the UI in

c) Gartner Peer Review on some SDNs for Datacentre

As Table III shows 34% of reviews related to Cisco ACI were from large enterprises, 38% from medium enterprises, 20% were from small enterprises, while 7% of reviewers were operating withing governmental establishments. VMWare NSX, 39% of the respondents were from large enterprises, 37% from medium sized enterprises, 13% from small enterprises and the remaining 11% were from government enterprises. Lastly, for Juniper Apstra, 60% of the respondent were from large enterprises while 20% were from small enterprises. It can be highlighted that large and medium sized enterprises have largely adopted SDN connectivity for datacenters in comparison to small enterprises.

Data gathered from the Gartner Peer reviews show the most common features within all SDN solutions are automation, centralized management, and security with several other features being vendor specific. In terms of cost, the solutions were not specific on their pricing. Prices were based on customer needs. Although especially for WANs and data centers, some respondents said that the SDN solutions were expensive, while some respondents stated the SD-WAN

solution was at a reduced cost in comparison to MPLS. The drawbacks were the fact that SDN has a steep learning curve, and the initial implementation is complex.

TABLE III. SDN SOLUTIONS FOR DATA CENTRE - GARTNER PEER INSIGHTS

Solution	Company size	Features	Cost	Drawbacks
Cisco ACI Data Centre (55 Reviews) [20]	Large Enterprise (34%) Medium Enterprise (38%) Small Enterprise (20%) Government Enterprise (7%)	-Automation & Central management, Security -Fast configuration -Stretching VLANs	Flexible Pricing based on need	-Complex to configure initially -Experience about instability with L2 bugs -Misconfiguration by Advance Services cause subnets flapping
VMWare NSX Data Centre (176 Reviews) [21]	Large Enterprise (39%) Medium Enterprise (37%) Small Enterprise (13%) Government Enterprise (11%)	-Automation & Central management -Management functionalities -Micro segmentation -Integrated load balancer -Security -Fast configuration	Flexible Pricing based on need	-The initial deployment is complex -Steep Learning curve -Lot of bugs in the platform -Complex product
JUNIPER APSTRA (5 Reviews) [22]	Large Enterprise (60%) Medium Enterprise (N/A) Small Enterprise (20%)	-Automation -Intent based networking -Multi-vendor support -Easy implementation -User friendly UI	N/A	-Some of their functionality is geared more toward service providers and hyperscale networks

2) Data collected from survey

A survey was conducted where a series of research questions were posed based on some of the questioning that was conducted within [31] and the Gartner Peer Insights review. There was a total of sixty-one (61) respondent majorly from various IT industries, managed service providers, telecommunication, internet service provider, energy company, financial institution, health sector, manufacturing, and consulting. Apart from the industry type, organizations were categorized by size to be able to deduce the category of respondent enterprise (Fig. 1). Organisations with 0-100 employees as small enterprise, 100 -999 employees as medium sized, and 1000 or above employees as large enterprises. Observe that over 50% of survey respondents were from large enterprises as shown in Fig 1. 31.91% from medium sized enterprises while 17.02% were from small enterprises. Even though most of our respondents are from large enterprises, the percentage of small and medium sized organisation is remarkable.

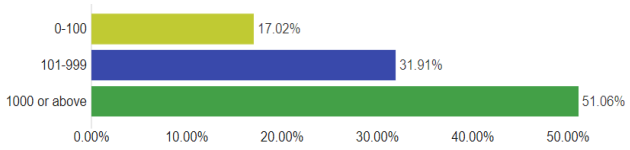

Fig. 1. Industry Size

Before the introduction of software defined networking, enterprises used a traditional networking approach. In the survey, 14.29% of the respondents were using traditional networking, the same 14.29% used SDN while the remaining 71.43% of the respondents used both traditional networking approach and SDN. This is an indication that a lot of enterprises are moving toward SDN (Fig. 2).

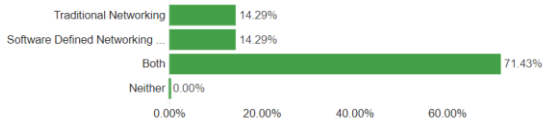

Fig. 2. Network Approach

Another critical part of the survey was discovering the context of deployment area of SDN within the respondent's organisation. Fig 3 shows that a larger percentage of the respondents used SDN in their WAN and data centres with 41.67% for data centres, 36.11% for WAN and 22.22% for campus network.

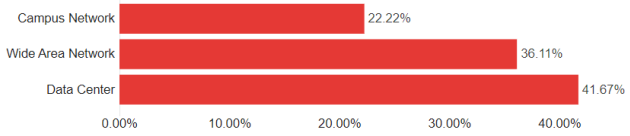

Fig. 3. SDN deployment area

Fig 4, 5 and 6 show the different SDN solutions used in different area of network based on the survey findings. For campus network, 40% of the respondents use Cisco SD Access, 22.86% use Cisco network service orchestrator, 8.57% use Juniper MIST while another 8.57% of the respondents use juniper SDN (contrail networking). A few others that consist of the remaining 20% of the respondent mentioned that they use Versa, Amazon Web Services, Azure, and universal CPE devices on an NFV.

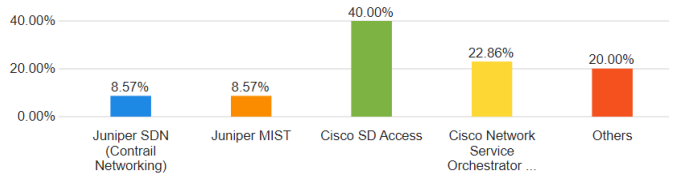

Fig. 4. SDN solutions for campus networks

Cisco Viptela and Cisco Meraki seems to be catching the attention here with each of them having 19.15%, after which we

have 17.02% respondent using VMware Velocloud, 10.64% use Fortinet SDWAN, 8.51% use Versa Networks, 6.38% use Palo Alto Prisma, another 6.38% use juniper solution while 2.13% use Extreme. Other Vendors mentioned here includes SDN NFV for delivery and Azure. For data centre solutions, 40% of respondents use Cisco ACI, 23% use VMware NSX,

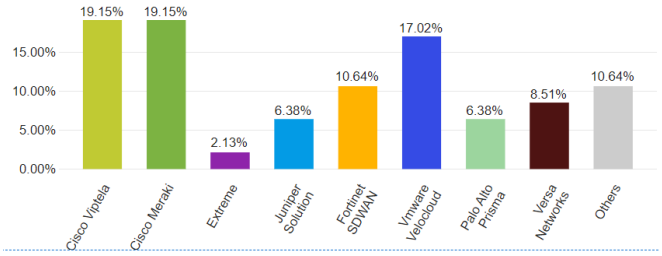

Fig. 5. SDN solutions for WAN

17% used Dell SDN solution, 9% uses Juniper APSTRA while HP and NUTANIX at 3% usage each.

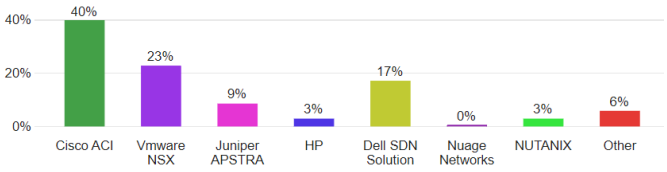

Fig. 6. SDN solutions for datacentres

It was of interest to find out enterprises using open-source solutions and what solutions they use. 67.74% of the respondents said they do not use open source, 22.58% said yes, they do but they did not mention the name of the solution, while the remaining 9.68%, mentioned that they use Python ansible, and a white box called universal CPE to spin different VMs.

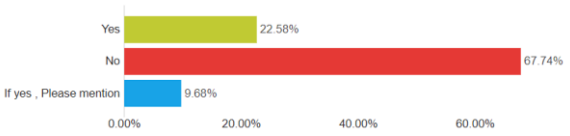

Fig. 7. SDN Open-Source Solution adoption

Guided by the drivers of SD-WAN deployment as stated in [33], it was of interest to find out what the major SDN drivers are from the perspective of our respondent. The survey result showed that enhancing overall business agility came first in order of importance with 54.84%, while reducing WAN management complexity, improving resilience and reliability, improving overall network performance, and improving business outcome were all second with 41.94% each. After that came "Ease of deployment" at the third place with 38.71%, then faster time to deploy in new location was fourth with 35.48%, while "it drives innovation" came fifth with 29.03% and lastly at the bottom of the list was reduced cost with 25.81%. This indicates that contrary to opinions in some previous literatures that cost reduction is a major SDN driver, even though reduced cost is important, organisations are not necessarily adopting SDN because of cost reduction but for many other benefits.

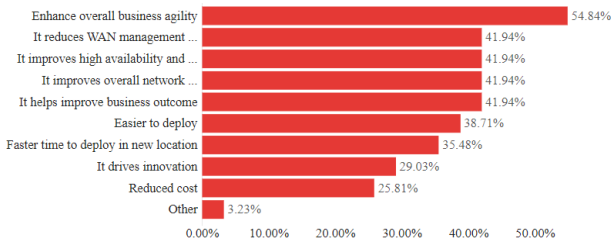

Fig. 8. SDN drivers and benefit

The following are the drawbacks indicated by respondents. 40.74% of respondents said it is expensive to deploy, 29.63% said it is difficult to implement while 25.93% said it is difficult to operate and manage. Other drawbacks mentioned by respondents includes new skill learning requirement, maintaining code base when there is high attrition rate, and low adoption rate.

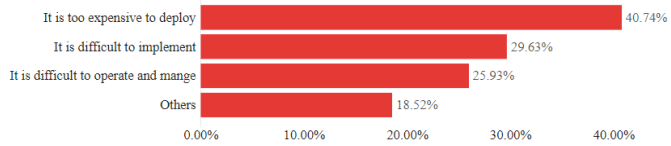

Fig. 9. SDN drawbacks

IV. Discussion and Conclusion

In this paper different SDN solutions for datacenters, WAN and campus networks were reviewed. Comparing the data gathered from the Gartner peer review, the independent survey and some part of 451-research report [31], the results look quite similar. As the result shows, it was found that datacenters seem to be adopting SDN much more than WAN, which seem to be next in line and then campus networks. All SDN solutions discussed in this paper have their various benefits and drawbacks as stated in the above findings. In terms of the features, automation, centralized management, and security were the common attribute of most of the vendors across board. One other key area worthy of note in the findings was the SDN drivers. Most of the respondents chose the business benefits of SDN such as enhancing overall business agility, reducing WAN management complexity, improving high availability and reliability, improving overall network performance, and improving business outcome over easier deployment, faster time to deploy, driving innovation, and reduced cost. Surprisingly, reduced cost was at the bottom of the list. These responses suggest that enterprises are mostly concerned about ensuring that their networks are optimized rather than just a reduction of cost. Looking at the network approach for most of our respondent gathered from the survey, over 71% used both traditional and software defined networking. This is an indication that organizations are gradually and strategically adopting the use of SDN. In terms of cost, there were no specific stipulated cost for the vendors. From the survey, many

respondents said SDN was expensive to deploy while some said the price was reasonable in comparison to MPLS. But indeed, most of these solutions does not have a fixed price as the costings largely depend on the business requirements and the SDN features required for a specific business. One major drawback that respondents mentioned especially for datacenters was the initial deployment complexity. This paper can serve as a guide to organizations intending to adopt a SDN solution. However, it is important to identify stakeholder requirement and bench mark these requirements with all available features, cost, drawbacks, and available support to be able to make a good selection decision.

REFERENCES

[1] Li, T., Chen, J., & Fu, H. (2019, April). Application scenarios based on SDN: an overview. In Journal of Physics: Conference Series (Vol. 1187, No. 5, p. 052067). IOP Publishing.

[2] Sezer, S., Scott-Hayward, S., Chouhan, P. K., Fraser, B., Lake, D., Finnegan, J., Vilijoen, N., Miller, M., & Rao, N. (2013). Are We Ready for SDN? Implementation Challenges for Software-Defined Networks. IEEE Communications Magazine, 51(7), 36-43. https://doi.org/10.1109/MCOM.2013.6553676

[3] Rana, D. S., Dhondiyal, S. A., & Chamoli, S. K. (2019). Software defined networking (SDN) challenges, issues and solution. International journal of computer sciences and engineering, 7(1), 884-889.

[4] Statistica, Software-defined networking (SDN) market size worldwide from 2021 to 2027, Retrieved from https://www.statista.com/statistics/468636/global-sdn-market-size/

[5] Hernandez-Valencia, E., Izzo, S., & Polonsky, B. (2015). How will NFV/SDN transform service provider OpEx? IEEE Network, 29(3), 60–67. https://doi.org/10.1109/MNET.2015.7113227

[6] NIST. (2012). The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology. In Public Cloud Computing: Security and Privacy Guidelines (pp. 97–101). U.S Department of Commerce.

[7] Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). Software-defined networking (SDN): a survey. Security and Communication Networks, 9(18), 5803–5833. https://doi.org/10.1002/sec.1737

[8] Jain, S., Kumar, A., Mandal, S., Ong, J., Poutievski, L., Singh, A., Venkata, S., Wanderer, J., Zhou, J., Zhu, M., Zolla, J., Hölzle, U., Stuart, S., & Vahdat, A. (2013). B4: Experience with a globally-deployed software defined WAN. Computer Communication Review, 43(4), 3–14. https://doi.org/10.1145/2534169.2486019

[9] Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015a). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14–76. https://doi.org/10.1109/JPROC.2014.2371999

[10] Gooley, J., Schuemann, D., Yanch, D., Curran, J. (2020). Cisco Software-Defined Wide Area Networks: Designing, Deploying and Securing Your Next Generation WAN with Cisco SD-WAN. United Kingdom: Cisco Press. ISBN-10: 0-13-653316-7, ISBN-13: 978-0-13-653316-0

[11] Cisco Systems Inc. (2020). Cisco Validated Design Program. https://www.cisco.com/c/en/us/solutions/enterprise/validated-design program/networking_solutions_products_genericcontent0900aecd80601e22.html

[12] Cisco. (2019). Cisco Application Centric Infrastructure (Cisco ACI). https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-741487.pdf

[13] Rotsos, C., King, D., Farshad, A., Bird, J., Fawcett, L., Georgalas, N., Gunkel, M., Shiomoto, K., Wang, A., Mauthe, A., Race, N., & Hutchison, D. (2017). Network service orchestration standardization: A technology survey. Computer Standards and Interfaces, 54, 203–215. https://doi.org/10.1016/J.CSI.2016.12.006

[14] Juniper Networks Inc. (2015). Contrail Architecture. https://www.juniper.net/content/dam/www/assets/white-papers/us/en/contrail-architecture.pdf

[15] Segec, P., Moravcik, M., Uratmova, J., Papan, J., & Yeremenko, O. (2020). SD-WAN- Architecture, functions and benefits. ICETA 2020 - 18th IEEE International Conference on Emerging eLearning Technologies and Applications, Proceedings, 593–599. https://doi.org/10.1109/ICETA51985.2020.9379257

[16] Cisco. (2022). Solution Overview: Cisco SD-WAN. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-sol-overview-cte-en.pdf

[17] Pratiwi, W., & Gunawan, D. (2021, July 7). Design and Strategy Deployment of SD-WAN Technology: In Indonesia (Case Study: PT. XYZ). 2021 International Conference on Green Energy, Computing and Sustainable Technology, GECOST 2021. https://doi.org/10.1109/GECOST52368.2021.9538796

[18] Cisco Meraki. (2023). MX - Cloud-Managed Security and SD-WAN. https://meraki.cisco.com/product-collateral/mx-family-datasheet/?file

[19] Cisco Meraki. (2022). Meraki SD-WAN Overview. https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MX_Security_and_SD-WAN/Meraki_SD-WAN

[20] Neupane, K., Haddad, R., & Chen, L. (2018). Next Generation Firewall for Network Security: A Survey. SoutheastCon 2018, 1–6. https://doi.org/10.1109/SECON.2018.8478973

[21] Fortinet Inc. (2022). Data Sheet: Fortinet Secure SD-WAN. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinet_secure_sdwan.pdf

[22] Palo Alto Networks. (2023). Prisma SD-WAN security architecture. https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/supporting/prisma-sd-wan/Prisma%20SD-WAN%20Security%20Architecture%20Whitepaper.pdf

[23] VMware Inc. (2013). NSX - Datasheet: VMware, Inc. http://www.vmware.com/go/patents.

[24] Badotra, S., & Panda, S. N. (2020). Evaluation and comparison of OpenDayLight and open networking operating system in software-defined networking. Cluster Computing, 23(2), 1281–1291. https://doi.org/10.1007/s10586-019-02996-0

[25] Asadollahi, S., & Goswami, B. (2018). Experimenting with scalability of floodlight controller in software defined networks. International Conference on Electrical, Electronics, Communication Computer Technologies and Optimization Techniques, ICEECCOT 2017, 2018-Janua, 288–292. https://doi.org/10.1109/ICEECCOT.2017.8284684

[26] Floodlight Project. (2018). Compatible Switches. https://floodlight.atlassian.net/wiki/spaces/floodlightcontroller/pages/1343519/Compatible+Switches

[27] Open Network Foundation. (2020). Administrator Guide - ONOS - Wiki. https://wiki.onosproject.org/display/ONOS/Administrator+Guide

[28] Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2014). Software-defined networking: A comprehensive survey.Proceedings of the IEEE, 103(1), 14-76.

[29] Haleplidis, E., Pentikousis, K., Denazis, S., Salim, J. H., Meyer, D., & Koufopavlou, O. (2015). Software-defined networking (SDN): Layers and architecture terminology. RFC 7426.

[30] Gartner Peer Insights Retrieved July 29, 2022, from https://www.gartner.com/peer-insights/home

[31] 451research Retrieved 2020 from https://451research.com/2020-trends

[32] Xing, T., Xiong, Z., Huang, D., & Medhi, D. (2014, November). SDNIPS: Enabling software-defined networking-based intrusion prevention system in clouds. In 10th International Conference on Network and Service Management (CNSM) and Workshop (pp. 308-311). IEEE.

[33] Eric H & Mike F, (2020), Software-Defined Networks are Creating New Challenges for Enterprise Security, Research 451, Retrieved July 28, 2022, from Palo Alto Networks : Software-Defined Networks are Creating New Challenges for Enterprise Security (hushly.com)

[34] Shirmarz, A., & Ghaffari, A. (2020). Performance issues and solutions in SDN-based data center: a survey. The Journal of Supercomputing, 76(10), 7545-7593.

[35] Thornley, P., Bagheri, M. (2021). Software-Defined Networking: Open-Source Alternatives for Small to Medium Sized Enterprises. In: Barolli, L., Woungang, I., Enokido, T. (eds) Advanced Information Networking and Applications. AINA 2021. Lecture Notes in Networks and Systems, vol 227. Springer, Cham. https://doi.org/10.1007/978-3-030-75078-7_20