# Security Analysis of SDN WAN Application - B4 and IWAN

Rajat jain
Fraunhofer SIT, TU Darmstadt
Darmstadt, Germany
Email: rajat.jain@stud.tu-darmstadt.de

***Abstract*—Software-defined WAN (SD-WAN) is specific SDN application designed to manage and deploy enterprise WAN networks. It's centralized controller feature helps to automate complex WAN configuration and efficiently route enterprise data among the remote sites. Banking on this architecture various big vendors have recently stepped in this market and claim their product to be the single solution to never seem ending WAN problems. However automating the network through a centralized controller makes network a handy target for attackers to exploit. Compromising the controller or its application can pose serious threat to network devices and traffic flow. In this paper we analyzed vulnerabilities of two such application Google's B4 and Cisco's IWAN using Microsoft's STRIDE model .We found out that both B4 and IWAN suffer from similar security threats like Spoofing, Tampering, Information Disclosure and Denial of Service. However, these threats can be tranquilized by today's IT security mechanisms. Additionally, for each vulnerability we specified the counter mitigation techniques to it.**

## I. Introduction

The data increment of IP applications over past few years have been alarming rising. According to study in [1] data usage will surpass zettabyte (i.e 1000 exabyte) in 2016. The result of which network management is becoming cumbersome and expensive for enterprise. On top of this, network teams are facing huge challenges to meet service levels for complex policies and mission critical application [1]. Many attempts are made in past to make network management easier, but the difficulty of changing underlying network always become major roadblocks to each of them [2]. In the same domain, SDN( software define networking) has projected the idea of seprating the control and data plane and orchestring the whole network through a centralized controller. Architecture claims that with the view of whole toplogy at single point will make the management easy and will cut down OPEX and CAPEX [2]. Figure 1 shows the basic architecture of SDN. It can be viewed as three layers. For understanding the architecture in detail the numbers are marked on the figure in increasing order to represent the flow of data. 1) Open flow [4] enabled switches using southbound interface sends the network update to the controller. 2) Controller collects the updates and prepares it for the applications. 3) Applications using northbound interface access the data and process it using its business logic. 4) Application forwards the instruction and updates the flow table at the controller. 5) Finally, controller using southbound interface updates the switches routing table.

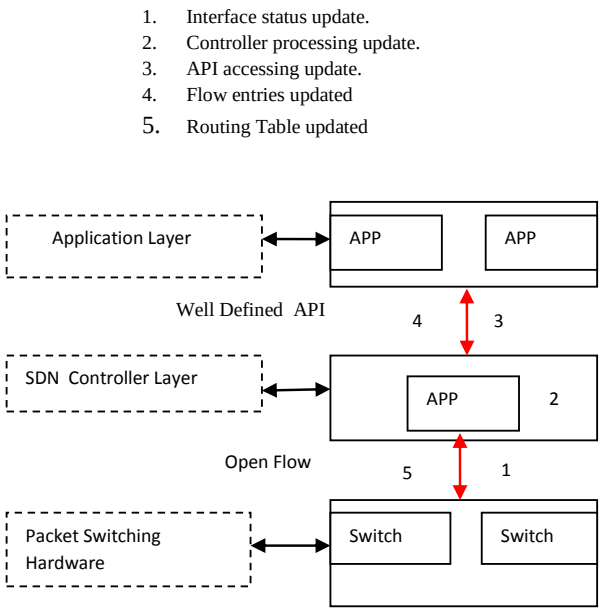


Fig. 1. Basic SDN Architecture and flow of data [5] (redrawn and modified1)

WAN management was always a big concern for organizations having multiple branches [5]. Over the past years, the organizations have invested a lot in their WAN infrastructure, but still face a huge challenge to manage QOS for business critical applications. Hybrid WAN somewhat has produced some relief in terms of cost but, its management has created whole new challenges for the network team [5]. Various vendor's SD-WAN products listed in table 1 enable hybrid WAN architecture. It allows enterprise to reduce cost by dynamically setting QOS and routing path of different classes of traffic over private and public links. Each of these applications have various security benefits which come with encryption in data plane and security in control plane [6]

For our study we decided to analyze B4 and IWAN. B4 is choosen because of its implementation in large data centers of Google and IWAN because it includes features like WASS, Application visibility and control and dynamic VPN creation that makes it a complete WAN management suite. The rest of the paper is structured as follows: Section 2 is an introduction to STRIDE and DFD. Section 3 and 4 presents application

TABLE I
VARIOUS SDN SOLUTIONS

| SDN | Vendor | Description | Area of Use | Security |
|---|---|---|---|---|
| IWAN [7] | Cisco | Virtual WAN, Intelligently routes based on priority, uses DMPVN cell5 | WAN | Firewall (Based on security rules) and Cloud-based (Security applications |
| ION [8] | Cloud Genix | SD-WAN, virtual elements on existing device acts as flow forwarders | WAN | Open Flow (SSL,TLS) and Cloud-based (Security applications |
| SEN[9] | Viptela | Delivers secure end-to-end virtualization for enterprise to build large scale network | WAN | Datagram TLS, IPSec |
| B4[10] | Google | Connecting data centers of Google worldwide | WAN | Open Flow (SSL,TLS) based |
| SDX [11] | Proto type | Software defined IXP | WAN | Open Flow (SSL,TLS) based |

introduction and security analysis and finally section 5 concludes the paper.

## II. APPLICATION THREAT MODELLING

Application threat model analysis is becoming the key part of product development for most organizations these days. It not only find the vulnerability in the product but also helps the team members to understand the product in much detail [12]. Moreover, threat model provides a structured display of causes that compromises the security of an application. General steps to follow for any threat modelling includes the creation of a structural overview of the application, splitting the application, identification of threats in each part and documentation of threats. Next phase includes prioritizing the threats, and last is to define mitigation techniques or tool.

Different schemes for identifying and classifying threats are developed over the years. Following are few of them listed along with their alignment to the study in paper.

*1) PASTA:* It is a simulation methodology suitable for designers and developers in the organization where the user needs to know the definition, technical scope of application and system from inside to work on threat analysis [13].

*2) Trike:* It is a threat modeling technique suitable for design phase as it is requirement centric and involves stakeholders. The trike is outdated now [14].

*3) Attack Tree:* It is available as open source as well as commercial software but it is attacker oriented than a system so not a good choice for entire system analysis [15].

*4) UMLSEC:* It is a more model-based approach where each component of the system is analyzed with various stereotypes which require knowing the source code which is our interest here [16].

*5) OCTAVE:* It is risk assessment tool for organizations where analysis team of expertise from various departments is required for analysis which makes it unsuitable for our analysis [17].

*6) Misuse Cases:* It is business process modeling tool based on the expert guidance of various fields like architecture, design, testing which is not possible here when we are analyzing the system alone [18].

*7) DREAD:* It is also used for risk assessment, but it is more subjective in nature when giving ratings to the threats and model itself is out-of-order [19].

*8) CORAS:* It is used for the organizational purpose as it needs customer interaction in security analysis which is out of scope for this paper [20].

### A. STRIDE

STRIDE is a methodology developed by Microsoft for identification and categorization of various threats in applications [21]. Initial letters of security threats like Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of Privileges forms STRIDE. According to [21], individual security threat is defined as follows.

**Spoofing of Identification** means pretending to authorize the user for accessing a certain service or application.
**Tampering with Data** involve unsanctioned manipulation of data. Change of data can be done during transmission or when it is not in transit.
**Repudiation** means denial of action after its occurrence. For example, user denies the truth that the action was performed by him.
**Disclosure** involves the leak of information to anyone, who are not authorized to access the information.
**Denial of Service** is the prevention of authorized user from accessing a service or application
**Elevation of Privileges** means that an ineligible user gets a privileged access to applications or services

For analyzing each security threat from the above STRIDE model, our application architecture needs to be represented by Data Flow Diagram (DFD). In DFD, we split our application into multiple components based on their functionality and

TABLE II
DFD COMPONENTS

| Component | Representation | Description |
|---|---|---|
| Data Flows | Arrow Represents | direction of flow of data |
| Data Stores | Parallel Horizontal lines | File database |
| Process | Circle | Application |
| Multi-process | Concentric Circle | Compilation of various subprocess |
| Interactors | Rectangle | It represents end-points which provides as well as consumes data in the system. |
| Trust Boundary | Straight Line (Dotted) | It is the boundary between trusted and untrusted components |

analyze the security threats for each component. Table 2 shows various DFD components, its representation, and description in accordance to [22]. Additionally, each component is vulnerable to a group of threats that needs to be addressed. Data flows and data stores are vulnerable to tampering, information disclosure and denial of service. Processes are vulnerable to all the threats. Whereas, interactors are vulnerable to spoofing and repudiation.

## III. B4

Google WAN network architecturally divided into two WANS. One for directing requests/responses and other for syncing users data across geographically distributed data centers named as B4. The requirement of QOS of traffic for both of these WAN networks are quite varied in nature. The user facing WAN is dense and require high bandwidth while the B4 requires high availability of data. Furthermore, the thousands of application which run over B4 requires a range of QOS classes. Some applications running on it are low in volume and demands low latency whereas some are high in volume and demands high bandwidth [11]. The cost of maintenance of these variety number of QOS classes and an end to end application control motivated Google to implement SDN technology. Figure 2 shows the basic architecture of B4. It can be viewed as three logical layers i.e Hardware, Controller, and Global. Hardware layer consists of commodity open flow switches. Controller layer consists of a cluster of NCS server for fault tolerance and an instance of Paxos which selects one NCS server as a master for the site. Each NCS server contains Open Flow controller (OFC) and Quagga. Quagga provides BGP connectivity between NCS servers and the gateway and exchange network and traffic engineering updates between them. OFC's RAP application subscribes to these Quagga's traffic engineering updates and forwards it to OFC. Finally, the global layer consists of gateway and topology server. Gateway connects multiple data center sites and topology server serves

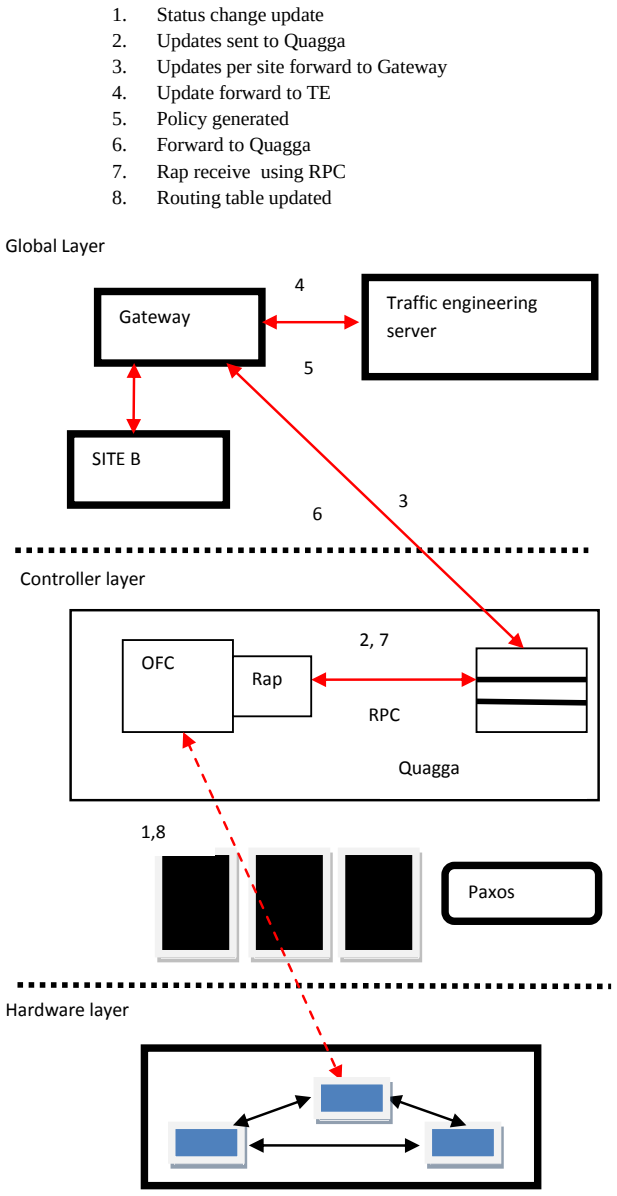


Fig. 2. B4 Architecture and flow of data [10] (redrawn and modified)

as the brain for the whole network. It define policies to engineers the traffic between these sites.

### A. Security Analysis

B4 uses the very basic routing technique. A general routing process is explained in Figure 2. The double red pointed lines denote the interface status change information communicated from the switch to the topology server and policies update back to the switch. 1) Open flow enabled switch sends the interface status information to the open flow controller in the NCS server 2) RAP SDN application forwards the information to the Quagga 3) Quagga using BGP update forwards the information to the Gateway 4) Gateway finally forwards the information to Traffic Engineering (TE) 5) TE having the full view of the network constructs a tunnel for application and

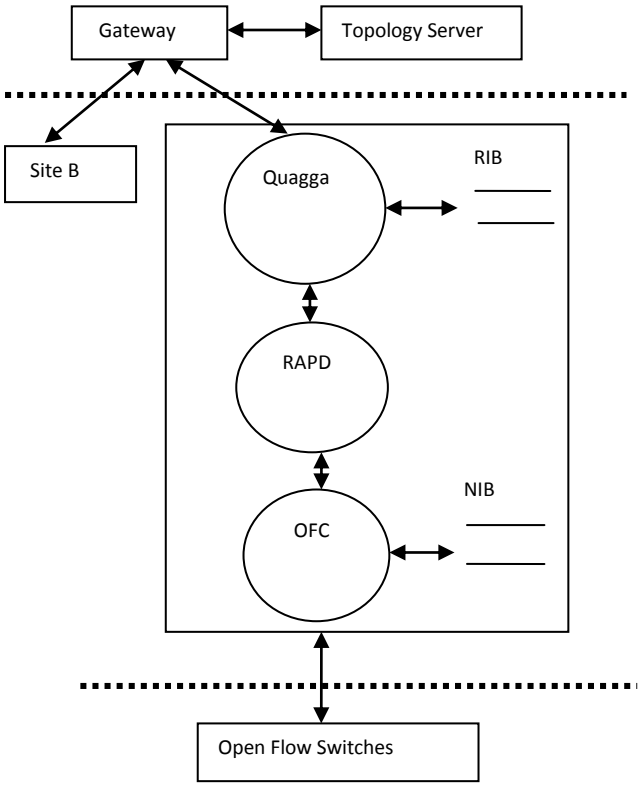


Fig. 3. B4 DFD

assigns a flow group to it and further floods this information to the Gateway. 6) Gateway simply using BGP updates pass the information to the Quagga 7) Rap is subscribed to the Quagga instructions using RPC, then it forwards the information to the OFC, using this OFC updates its flow table (NIB) 8) Finally information is flooded to the switches which updates their routing table.

For analyzing the security features of B4 we followed the steps mentioned in section 2. For DFD of the above scenario, the application basically is decomposed into four main components on behalf of production and consumption of data. Topology server, NCS server, Topology server and Open Flow hardware switches are those four and are considered as interactors for the DFD. Each NCS is hosting OFC, Quagga and two databases Routing information database (RIB) and Network information database (NIB). Including RAP application Quagga and OFC are considered as processes and two databases as data stores. The two-way data flows is specified according to the interaction of data with each DFD components in the graphical representation of DFD in Figure 3. Additionally, there are two trust boundaries. Branch Switches are kept outside trusted boundary because they can't inherently be trusted. Gateway and the central TE server outside as well because gateway is orchestration point of multiple data center sites any adversary present in one of the site can attack the resources of other.

*1) Data flows:* Data flow is vulnerable to tampering, information disclosure, and denial of service which leads to attack on integrity, confidentiality, and availability of data. If not secured it can further compromise the processes and data stores which process and store the flow. Data flow from switches to the gateway and vice versa passes through the controller which makes it much more important to be secured. Switches lie outside the trusted zone but uses Open Flow protocol for communicating with OFC. Open Flow is inherently secure as it uses Transport Layer Security (TLS) for securing communication [4]. It protects from tampering of data and information disclosure by encrypting the data. It uses public key cryptography, that ensures a private communication between the entities. Switches and controller are in isolated management plane so kind of immune to denial of service attack but still to make it more secure throttling filtering or QOS mechanism can be implemented [22]. The data flow between gateway and NCS server and between gateway and Topology server are vulnerable to all the three threats. Tampering and information disclosure can be mitigated by using encryption and message integrity check mechanism. Whereas, denial of service can be prevented by throttling mechanism or QoS. Data flows inside the NCS server between Quagga and RAP or RAP and OFC are inherently considered to be secured.

*2) Data store:* Data stores are vulnerable to tampering, information disclosure and denial of service. In B4 data is stored in RIB, NIB. Compromising security of any of these data stores would result in the vulnerability of the whole system. However, both these data stores are considered to present locally inside the NCS Servers so can only be attacked if NCS server is compromised hence inherently considered secure.

*3) Process:* Processes are vulnerable to all six threats though for processes RAPD, OFC spoofing, tampering and information disclosure can be neglected as they are present in the same server thus inherently can be trusted. However both processes are vulnerable to repudiation attack. This can be prevented by maintaining a log file with entries of each communication stored in it for later analysis. For mitigating elevation of privileges attack the process must be run with the minimum required privileges and for protecting against DoS attack users must be authenticated and authorized and throttling or filtering of user request reaching to the process must be considered.

*4) Interactors:* Interactors are prone to spoofing and repudiation. In our DFD, switches, NCS Server, Gateway and TE server are the interactors. Switches and NCS servers consider safe from both these attacks as they both use TLS enabled communication between them. Gateways and TE server can be spoofed if one is able to get access to the shell of an interactor. He/she can push certain commands which can bring the application to a halt. In order to protect from such attack shell access must be authenticated and authorized. For example usage of AAA server in the network can mitigate such attacks. AAA stands for authentication, authorization, and accounting AAA accounting feature will log each and every activity of user so any malicious attempt made by the user can be easily traced back to him thus it mitigate repudiation attack.

TABLE III
STRIDE MATRIX OF B4 WHERE" M" SHOWS THREAT MITIGATION TECHNIQUE SUGGESTED IN PAPER, "*" INDICATES THREAT MITIGATED BY THE APPLICATION ARCHITECTURE," -" REPRESENT THREATS OMITTED. "G" REPRESENT GATEWAY," T" IS TOPOLOGY SERVER, "N" IS NCS SERVER, S IS SWITCHES AND "=" REPRESENT TWO WAY FLOW

| Threat | Interactor | | | | Process | | | Data Flows | | | | | Data Stores | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | G | T | N | S | OFC | RAP | Quagga | G= Quagga | OFC = S | OFC = NIB | OFC = RIB | G = T | NIB | RIB |
| Spoofing | M | M | * | * | * | * | * | - | - | - | - | - | - | - |
| Tampering | - | - | - | - | * | * | * | M | * | * | * | M | * | * |
| Repudiation | M | M * | * | M | M | - | | - | - | - | - | - | - | |
| Information Disclosure | - | - | - | - | * | * | * | M | * | * | * | M | * | * |
| Denial of Service | - | - | - | - | M | M | M | M | M | * | * | M | * | * |
| Elevation of Privileges | - | - | - | - | M | M | M | - | - | - | - | - | - | - |

Summary of threat analysis is shown in Table 3.

## IV. IWAN

Cisco IWAN is one of the Cisco APIC EM controller application developed for hybrid WAN management using SDN technology. It supplies all the capabilities of WAN management such as WAN optimization, performance routing and deep packet inspection and VPN tunneling in one suite. IWAN makes it possible to route enterprise traffic smoothly on both private expensive WAN connection and on less expensive internet transport [23]. IWAN helps the organization build dynamic multipoint VPNS (DMVPN) with zero touch deployment and intelligently route encrypted application traffic independent of WAN transport. Additionally, it optimizes the WAN link using Cisco WASS and secure communication using Cisco cloud security. It basically summed up as has four features. 1) Transport Independent Design. 2) Intelligent Path Control 3) Application Optimization 4) Secure Connectivity

### A. Security Analysis

The working of IWAN is explained using a basic scenario in Figure 4. In the nutshell, headquarter (Hub) is sending business critical traffic to private cloud using MPLS private link and in during the certain time of the day private link get congested then Cisco IWAN dynamically picks the low priority data from the private link and re-route to internet link. For our study we assumed initial performance based routing policies for the application is already configured on the border and master router 1) Headquarter starts sending the application stream 2) Border router using NBAR2 start deep inspecting the stream of packets. 3) Border router collects the metrics such as link utilization and throughput of application over private WAN link then using Net flow V9 sends traffic to the master router. 4) IWAN starts collecting the traffic metrics from the master. 5) Seeing the traffic metrics reaching threshold IWAN instructs the master router to re-route the low priority applications running on private WAN link to the other WAN link (internet). Controller will keep a sharp look on any further change in metrics and change policies according to that.

For security analysis of IWAN we followed the same steps as we did for B4. We first define the DFD (Figure 5) then analyze it using Stride. Basically architecture can be decomposed into four main component groups that are one or more LAN switch, Cisco APIC EM controller, master router and both Border routers. Each of these group is considered as interactors. The scenario in Figure 4 reveals LAN and master router, master router and border route, border router and cloud and master router and IWAN communicate with each other. This communication is modelled as data flow. Furthermore, AVC, PFR, and WASS running on border router and IWAN on APIC-EM controller are considered as processes. Finally, there are two trust boundaries. Branch switches are kept outside the trust boundary because users connected to the switches can't be trusted as they can overhaul the link between the master router and border router with bogus traffic which can hamper the IWAN performance. Second trust boundary is between edge router of the organization and WAN link. Data and users from the WAN link can't be trusted either. There are no data stores for this application.

*1) Data flow:* Data flow is vulnerable to tampering, information disclosure, and denial of service which leads to attack on integrity, confidentiality and availability of data according to stride model. Information disclosure attack on the flow between master and border routers can be performed by tapping the network between them but it is hard to achieve as it traverses only one link. No specification is given in [23] but still to have confidentiality of data use of IP sec tunnel

1. Business traffic from LAN
2. Master router Route using predefined policies
3. Traffic passed to cloud (MPLS link)
4. Net flow traffic metrics
5. Metrics passed to IWAN
6. New policies instruction
7. Traffic redirected to other WAN
8. Traffic passed to cloud

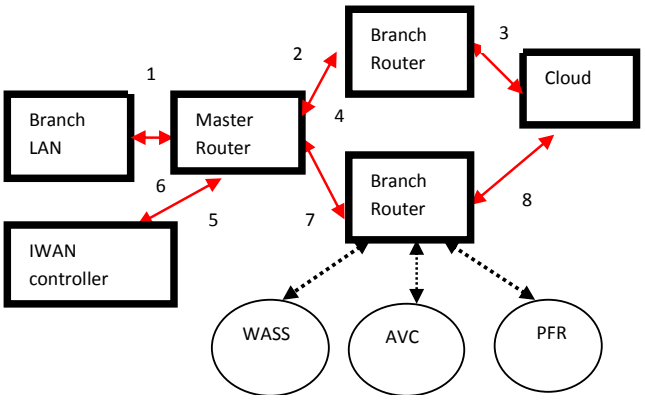


Fig. 4. IWAN Architecture and flow of data [23] (redrawn and modified

between the routers can mitigate this. Similarly data can only be tampered if the attacker is able to tap the network and spoof TCP packets.This can also be mitigated using IPsec tunnel. Denial of service attack on this flow can be performed if malicious user attached to the branch LAN sends bogus traffic and overloads the link between the routers. To mitigate this authentication, authorization of users attached to LAN and adjusting the QOS of routing protocol packets and data metrics mechanisms can be used.

Data flow between controller and master router is immune to both tampering and information disclosure attack. Both these interactor uses Open flow protocol between them for communication which is TLS enabled [4]. Controller and master router communication is in isolated data plane this provides immunity to Denial of Service attack. But still, link can be exhausted by sending the large number of Open Flow request to the controller. This kind of attack can be mitigated using either QOS, filtering or throttling mechanism [22].

Data flow between branch LAN and the master router is prone to all three attacks. Denial of service threat can be omitted as unavailability of LAN is not a concern of IWAN. Whereas attacker with tampering and information disclosure attack can manipulate and judge the traffic and with spoofing himself/herself it can send bogus traffic on the WAN link which can make IWAN to alter the configuration. This is mitigated using TLS between LAN and master router and authenticating and authorizing users on LAN. The flow of data from branch routers to the internet is immune to tampering and information disclosure attack because of IP sec IKE2 encryption [24]. Whereas the DoS attack can surely hamper the working of IWAN. Unavailability to pass data through one link will cause the IWAN to change the policies and routing

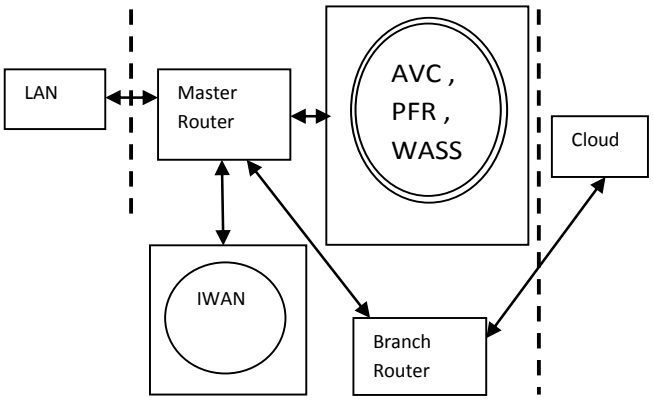


Fig. 5. IWAN DFD

entry on the master router which can make the possibility of sending business critical data on the less secure internet link. To protect either use dynamic IP on WAN ports of branch routers or prioritize the business critical data on private WAN link.

*2) Interactors:* are prone to spoofing and repudiation. In our DFD, Master router, Border router Controller and LAN switches are interactors. Spoofing attack on the switch can be performed if the attacker attached to switch port congest the WAN link with bogus traffic which can make a controller alter the policies on the master router. It can be protected either by setting edge ports to static access or disable DTP auto-negotiation [25]. Repudiation attack on the switch can be prevented by using synchronized Syslog [26] entries on the switch and authenticating the user connected to switch using AAA [27]. IWAN controller and master router are both immune to tampering and repudiation attack because of open flow TLS feature. On Border routers, spoofing attack can be performed if console or management passwords are compromised. Cisco OS access is generally protected through AAA server which accounts, authenticates and authorize activity on the router. DMVPN IPsec tunnel uses RSA signature as one of the three options for authentication of end point of the tunnel this provides immunity to repudiation attacks [28].

*3) Process:* As per STRIDE model, the process is vulnerable to all six threats. In scenario, there are four processes WASS, AVC, PFR, and IWAN App. Attacks will only be possible if hardware comprising these processes get compromised. In the case of AVC, WASS, PFR if border routers are compromised then the only attacker will be able to execute further attacks. Spoofing and tampering of the process can be performed by modifying the Cisco OS (Cisco-Xe for routers and APIC EM for the controller) binary image. It is done by adding malware to Cisco OS. This is protected by using Cisco Image Verification feature. It is built on the MD5 file validation and it ensures any corruption to OS image functionality to network administrators. Furthermore, security of OS can be improved by providing authorization to the certain user for commands like config-register, show memory etc [29].

Information disclosure attack can be possible if the attacker

TABLE IV
STRIDE MATRIX OF IWAN WHERE" M" SHOWS THREAT MITIGATION TECHNIQUE SUGGESTED IN PAPER, "*" INDICATES THREAT MITIGATED BY THE APPLICATION ARCHITECTURE," -" REPRESENT THREATS OMITTED. "LAN" REPRESENT BRANCH," CONT" IS CONTROLLER, "M.R" IS MASTER ROUTER, "B.R" IS BORDER ROUTER AND "=" REPRESENT TWO WAY FLOW

| Threat | Interactor | | | | Process | | | | Data Flows | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | LAN | Cont | M. R | B. R | AVC | PFR | WASS | IWAN | LAN = M.R | M.R = Cont | M.R = B.R | B.R = WAN |
| Spoofing | M | * | * | M | M | M | M | M | - | - | - | - |
| Tampering | - | - | - | - | M | M | M | M | M | * | * | * |
| Repudiation | M | * | * | * | M | M | M | M | - | - | - | - |
| Information Disclosure | - | - | - | - | M | M | M | M | M | * | * | * |
| Denial of Service | - | - | - | - | M | M | M | * | - | M | M | M |
| Elevation of privileges | - | - | - | - | M | M | M | M | - | - | - | - |

is able to get its hand on the binary image of OS and it performs static and dynamic code analysis. By performing code analysis he/she will again the knowledge of the flow of data in the application [30]. Using such knowledge he can alter the flow of data which can bring the WAN application to halt. This can be protected by encrypting the binary file. In this scenario, an attacker from branch LAN can perform DoS attack on all process except IWAN by sending bogus data to overwhelm the router OS which can halt the AVC, PFR, and WASS process. It can be mitigated using Cisco Copp [29] or ACL for filtering the unwanted/malicious traffic coming to the router control plane. IWAN is immune to this attack as controller lies in the isolated management plane. Elevation of privileges on all process can be mitigated by running each process with least privileges. Summary of the threats are shown in Table 4.

## V. CONCLUSION

This paper includes the motivation for applying SDN to WAN networks additionally, enumerating various software dened WAN application for their security analysis. Variable domain of B4 which is implemented in data center and IWAN for its complete WAN suite motivated us for selecting these two WAN architectures for security analysis. Security analysis includes decomposing the application architecture into various components using data ow diagram and analyze the security threat of each component using STRIDE methodology. Study suggest both application suffers from some security vulnerabilities and these can be mitigated using existing security mechanism. Additionally, both the application use Open Flow protocol for communicating controller with external hardware which inherently consider secure to spoofing tampering and repudiation attack because of presence of TLS. Therefore to protect from above three threats TLS needs to be implemented. Moreover, for the prevention of denial of service attack throttling, filtering mechanisms can be used. By implementing the above mitigation techniques future software dened WAN will become more secure.

## REFERENCES


[1] The Zettabyte Era Trends and Analysis. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/serviceprovider/visual-networking-indexvni / VNI Hyperconnectivity WP. html (accessed on 27/07/2016).

[2] W. Stallings Software Dened Networks and OpenFlow. [Online]. Available: http://www.cisco.com/web/ about/ac123/ac147/archived issues/ipj 16-1/161 sdn. html (accessed on 27/07/2016)

[3] Software-Dened Networking: Why We Like It and How We Are Building On It. [Online]. Available:http://www. cisco.com/c/dam/en us/solutions/industries/docs/ gov/cis13090 sdn sled white paper.pdf (accessed on 29/7/2016)

[4] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, OpenFlow: Enabling innovation in campus networks, ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 6974, 2008

[5] D.Jacobs, How software-dened WAN architecture is changing themarket.[Online].Available:http://searchsdn.techtarget.com/tip/How-softwaredenedWAN-architecture-is-changinthe market(accessed on 02/01/2016).

[6] J. Dix, The rst place to tackle SDN: in the WAN. [Online]. Available: http://www.networkworld.com/ article/2873964/sdn/the-rst-place-to-tackle-sdn-inthe-wan.html?page=2 (accessed on 02/01/2016).

[7] Cisco Intelligent WAN. [Online]. Available: http://www Cisco. com / c / en / us / solutions / enterprise - networks / intelligent-WAN/index. html (accessed on 03/02/2016)

[8] Software-defined WAN: More uptime for your network, more downtime for you.[Online]. Available: http : / / www . cloudgenix . com / software-defined wan/ (accessed on 03/02/2016).

[9] Secure Extensible Network (SEN) Solution. [Online]. Available: http://VIP tea.com/ solutions / overview/ (accessed on 03/02/2016).

[10] S. Jain, M. Zhu, J. Zolla, U. Holzle, S. Stuart, A. Vahdat, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. WANderer, and J. Zhou, B4: Experience with a globally-deployed software defined WAN, in ACM SIGCOMM Computer Communication Review, ACM, vol. 43, 2013, pp. 314.

[11] N. Feamster, J. Rexford, S. Shenker, R. Clark, R. Hutchins, D. Levin, and J. Bailey, SDX: A software-defined internet exchange, Open Networking Summit, 2013.

[12] Microsoft, Improving Web Application Security: Threats and Countermeasures. [Online]. Available: https : / / msdn . microsoft . com / en - us / library / ff648644 . aspx (accessed on 02/01/2016).

[13] T. UcedaVelez, Real World Threat Modeling Using the PASTA Methodology, OWASP App Sec EU 2012
[14] P Saitta, B Larcom, M Eddington,Trike v.1 methodologydocument[draft], URL:http://dymaxion. org/trike/Trike pdf,2005
[15] Bruce Schneier Attack trees, Dr. Dobb's journal, 1999
[16] Jan Jrjens, UMLsec: Extending UML for Secure SystEMs Development, J. -M. J ez equel, H. Hussmann,S. Cook (Eds. ): UML 2002, LNCS 2460, pp. 412425, 2002. cSpringer-Verlag Berlin Heidelberg 2002
[17] Christopher Alberts,Audrey Dorofee,James Stevens,Carol Woody, Introduction to the OCTAVEApproach. Pittsburgh, PA 15213-3890 : Carnegie Mellon University, August 2003Pittsburgh, PA 15213-3890 : Carnegie Mellon University, August 2003
[18] Misuse Cases.[Online].Available:http://ro.ecu.edu.au/cgi/viewcontent.cgi ?article=1119 contextism (accessed on 29/07/2016).
[19] Qualitative Risk Analysis with the DREAD Model, http://resources .infosecinstitute. com/qualitative-risk-analysis-dread-model/ Posted in General Security on May 21, 2014
[20] The CORAS approach to model- driven risk analysis. [Online]. Available: https://securitylab.disi.unitn.it/lib/exe/fetch.php.
[21] M. N. Johnstone, Threat modelling with STRIDE and UML, 2010.
[22] M. Tasch, R. Khondoker, R. Marx, and K. Bayarou, Security Analysis of Security Applications for Soft-ware Defined Networks, in Proceedings of the AINTEC 2014, ACM, 2014, p. 23.
[23] Cisco Intelligent WAN Design Guide. [Online]. Available: http://www.cisco.com/c/dam/en/us/td/docs/solutions/ CVD/Jan2015/CVD-IWANDesignGuide-JAN15.pdf (accessed on 29/07/2016)
[24] An Introduction to IP Security (IPSec) Encryption [Online]. Available: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/16439-IPSECpart8.html(accessed on 29/07/2016).
[25] Dynamic trunking protocol. [Online]. Available: http://www.cisco.com/c/en/us/tech/lan-switching/dynamic-trunking-protocol-dtp/index.html (accessed on 29/07/2016).
[26] Cisco OS Synchronized Logs: Syslog. [Online]. Available: http://www.cisco.com/c/en/us/tech/ip/syslog/index.html(accessed on 29/07/2016).
[27] TACAS: Accounting, Authorization, Acconting. [Online]. Available: http://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html (accessed on 29/07/2016).
[28] IPSEC RSA negotiation. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/iosxml/ios/ configuration/xe-3s/sec-ike-for-ipsec-vpns-xe-3s-book/sec-key-exch-ipsec.htm l (accessed on 29/07/2016).
[29] Cisco IOS Security. [Online]. Available :http://www.cisco.com/c/en/us/about/security-center/integrity-assurance.html (accessed on 29/07/2016).
[30] Cisco Control Plane Policy. [Online]. Available: http://www.cisco.com/c/en/us/about/security-center/copp-best-practices.html (accessed on 29/07/2016).