Securing East-West Communication in Clustered Multi-SDN Controller Network

Sarada Hettiarachchi
www.edsarada.com

Abstract

It is required to implement a robust reliable flow securing approach in a Multi-SDN controller environment with the available SDN controller application.

IPSec protocol has used to implement the security between forwarding devices and the South bound of controller with OpenFlow. Therefore, similar type of approach to secure East – West communication in between controllers will open many research avenues in the future. This research paper has challenged to implement such security using the most suitable protocol.

Introduction

Software Defined Networking (SDN) is the next generation networking approach, which uses centralized software controller to manage network operations. This approach is very new to the industry as well as to the academia.

The Software Defined Networking approach replaced the individual control plane of each hardware to common centralized dedicated hardware for that purpose. The SDN controller will manage data flow and network control communication with more visibility of the entire network.

However, this approach will lead to single point of failure, in the event of communication failure between network hardware and SDN controller. Therefore, many researches are going on to design and implement multi SDN controller environment to the enterprise and Internet Service Provider (ISP) networks with centrally configurable platform. Multi SDN controllers are highly important not only because of single point of failure, but also for load sharing purposes in branch to central office networks and Service Provider to customer connectivity. Therefore, the academia has being conducting many researches to produce centrally configurable multi SDN controllers over Wide Area Networks (WAN). In addition to that, it is highly vulnerable to communicate between SDN controllers via public WAN connections and many incidents have reported about SDN flow attacks. Therefore, secured SDN controller communication over public WAN is highly important.

This research paper focus to secured communication between multi SDN controllers over the public WAN connections. The possibility to integrate IPSec protocol suite researched throughout this effort. There are different avenues to conduct different researches to accomplish this objective based on the current and future requirements. Therefore, this could be a stepping-stone for valuable future research work on secured SDN controller communication over WAN.

SDN Controller

SDN controller is an application, which controls the entire SDN network. In other terms, SDN controller is the "brain" of the SDN network.

Mainly, there two major components in the SDN controller software. Southbound API component will communicate with the forwarding plane devices and North bound API component will communicate with the application software running on top of the SDN controller to manage control plane policies.

Most of the existing SDN enterprise networks are operating with single SDN controller. In addition to that, most of the vendors are in the development face of their SDN controllers to improve their controllers to Multi-SDN controller environments.

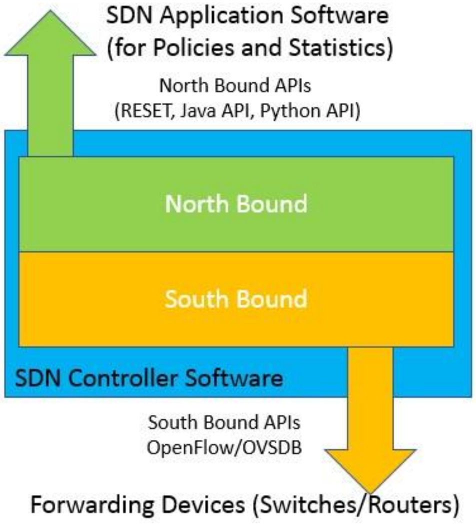

Figure 1 - SDN Controller overview

The Multi-SDN controller environment will provide redundancy and more resilient network for large organizations. Especially, Service Provider networks (SDWAN) will be benefitted in many ways in terms of cost, visibility and resiliency.

North bound and Southbound communication are considered in a single SDN controller. However, in the Multi-SDN controller environment East-West communication also available for the horizontal connectivity.

Multiple SDN controller environment is essentials with centrally configurable platform.

However, if there are distributed multiple SDN controllers available in the network, following critical security concerns are inherited.

- The Multi-SDN Controller environment over the public WAN connections, unintended flow communication can happen.
- Flow leakages will provide information to the intruders to produce flow-based DDoS attacks.
- Plan text flow information communication over the WAN is highly vulnerable.
- Simple authentication protocols are not suitable to secure flow information flowing through public WAN connections.
- Vendor specific protocol or protocol suite to implement the flow security will not provide the sustainability for future enhancements.

East – West communication in distributed SDN

Southbound communication will accomplish through standards protocols like OpenFlow or Open Virtual Switch Database Management. Northbound communication will fulfil via different sets of standards APIs. However, there are very few researches discussed about the horizontal communication between SDN controllers. There is no such standard approach and protocol have facilitated to implement better East – West communication. In other terms, it is the Control Plane to Control Plane communication.

Most crucial factor in a multi SDN controller is the possibility to maintain the shared state of the configuration between each server identically. Event during the failure and after reconnecting them, this is critical matter.

distributed SDN controller architecture is highly suitable for large organization to manage their branch SDNs. However, logical centralization need to maintain for centrally configurable common control plane of the network. In addition to that, load balancing and process sharing can efficiently functional with the distributed architecture.

However, interconnecting SDN with distributed architecture for geographically sperate SDN environment will produce high security considerations to safeguard the flow communication.

Most crucial factor in a multi SDN controller is the possibility to maintain the shared state of the configuration between each server identically. Event during the failure and after reconnecting them, this is critical matter.

Mainly, there are two algorithms used for this horizontal communication in SDN controllers.

1. Raft Consensus Algorithm
2. Anti-Entropy algorithm

Raft Consensus Algorithm

Raft is good in log replicating with multiple servers in parallelly. It consists of safety, high availability, no time dependent and majority makes decisions properties to maintain the consistency of the group of SDN controllers.

Before the operation starts, the algorithm itself will elect a leader, which manages all the replicated entries. all the followers will send information the leader to replicate with other devices. Followers are in passive mode. However, there is another statement in the algorithm as Candidate. If the followers do not get periodic heartbeat from the leader, then leader election will happen. During the election, all the followers become candidates and until one candidate wins the election will happen (Ongaro, 2014).

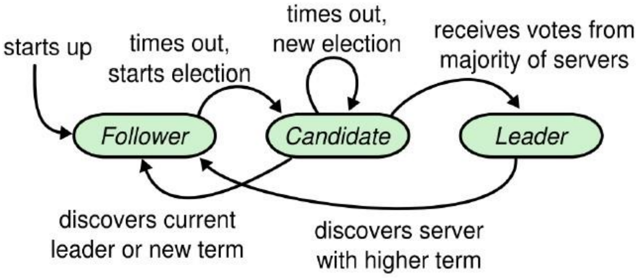
starts up
times out, starts election
times out, new election
receives votes from majority of servers
Follower
Candidate
Leader
discovers current leader or new term
discovers server with higher term

Figure 2 - Raft election

Anti-Entropy algorithm

This is the second algorithm type, which uses to horizontal communication between SDN controllers. This algorithm will store all the updates in the primary controller and propagate to randomly selected control in every five ms. therefore, commonly identified that it runs with gossip algorithms.

The synchronization communication will send the information about flow switches, links and host connected in the current topology. In addition to them, very recently removed elements called "tombstones" information also communicated. This algorithm is time dependent and most recent update will overwrite the previous update.

In this algorithm, there is no centrally controlled communication procedures and it is most likely Peer-to-Peer approach (Tianzhu Zhang, 2017).

Table 1 - Algorithm Comparison

	Strong Consistency	**Eventually Consistency**
Data Structure	Consistent Map	Eventually Consistent Map
Algorithm	RAFT	Gossip
Update Period	Instant	Periodically (5ms)

Security vulnerabilities in the horizontal communication between clustered SDN controllers

Due to the centralization of the control plane in the SDN environments, there are many inherited security vulnerabilities existing with the technology. Vulnerabilities can be categorized in to Control plane and Link vulnerabilities.

Some of these vulnerabilities are having very high threat level in a multi SDN environment. In addition to that, multi SDN over wide Area Network will increase the possibility to experience higher number of incidents. **Control Plane vulnerabilities**

Mainly, there are two types of vulnerabilities exist under the level of control plan operations.

1. DDoS to the controllers
2. Controller compromising

Single point of administration of SDN environment is the SDN controller. Therefore, Distributed Denial of Service (DDoS) attack can manipulate SDN controllers to exceed the limit of flow table capacity. Nevertheless, in a clustered environment, single compromised SDN controller can use to manipulate all the other SDN controllers in the network. A network with single SDN controller will experience resource starvation and single point of failure in the event of DDoS attack. **Link level vulnerabilities**

the unencrypted communication over the SDN controllers in the East-West communication that communication susceptible to a vulnerability like man-in-the-middle attack. The attacker can eavesdrop to the configurations and policy information in the distributed network. This information leakage will lead to fabricate falsify policy information and that can circulate legitimately over the distributed SDN controllers. Through this approach, the intruder can get the accessibility to the forwarding plane devices also.

Though it is encrypted control message communication among the distributed SDN controllers, the proper data integrity in the communication should implement. If there is no proper mechanism to identify the past and present communication, in future there can be replay attacks.

Out of all the above attack types, centrally configurable distributed SDN controller environment will produce more attacks on link level.

Existing approaches in SDN controllers to secure east-west communication

There is very less research works conducted on this area. However, there are research approached to secure the east – west boundaries through Identity-Based Cryptography (IBC) protocol (Jun-Huy Lam, 2015). This approach proposed to secure the east west on top of the SDN controller application. Furthermore, the approach has less considered the SDN controller’s operating systems (OS) level communication security.

Though SDN controller software is a network application, it is highly recommended to implement a security solution to cover maximum number of layers in the OSI reference model. Furthermore, it is highly required to minimize link level vulnerabilities.

There are two main protocol structures can be used to implement the East-West SDN communication.

1. IPSec protocol stack
2. TLS/SSL protocol

IPSec Protocol for Multi SDN Controller Security

IPSec is coming under RFC 2401-2412 and it an IETF standard. This protocol suite will provide the facility to secure the IP networks. IPSec suite will protect and authenticate source and destination connectivity via Internet Protocol. Furthermore, IPSec is having the capability secure no IP traffic as well.

Confidentiality, Integrity, Authentication and Secure key exchange are key functionalities in the IPSec.

However, IPSec is not a rigid protocol suite with restricted or limited to selected protocols. it is a protocol suite which supports to multiple protocols in various levels.

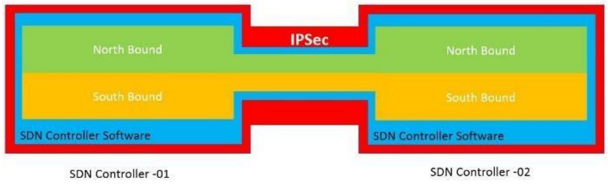

Figure 3 - Secured Distributed SDN Controllers

TLS for Multi SDN controller security

Transport Layer Security (TLS – RFC 2246) is based on SSLv3. It is a Layer 4 protocol as it runs directly on top of TCP only. It uses PKI to provide user authentication as well as symmetric keying for confidentiality protection.

There are two types of authentication mechanism in TLS.

1. Mutual Authentication
2. Server-Side Authentication

Both mechanisms are depending on the certificate authentication. In Mutual Authentication, bi directional validation of certificates will provide the acceptable security for a SDN clustered network. However, this approach is required PKI (Public Key Infrastructure) in both ends. This requirement will produce high process intensive activities in SDN controllers to implement TLS Mutual Authentication.

In Server-Side-Authentication, one side authentication will be happened, and this approach produces client-server architecture in terms of security in the SDN cluster while the SDN controllers operate as server-to-server architecture in the SDN environment.

Conclusion

The East West security of multi Software Defined Network controller environment is very new to the industry and academia due it's freshness of the technology.

However, according to the above two approaches, IPSec is producing from Layer 3 to Layer 7 (OSI) security through its multi-protocol stack comparing to TLS.

Furthermore, IPSec is having the capability to establish, Point-to-Multipoint tunnels from the Operating System (OS) level.

Therefore, IPSec protocol is the best selection not only for the forwarding plan security, but also it can use for the control plane security in a clustered SDN environment.

Reference

Affan Basalamah, E. M., 2015. *SDN & Cloud Related Activities & Research.* [Online] Available at: https://www.slideshare.net/IDNOG/07-idnog02sdn-research-activity-in-institut-teknologibandung-by-affan-basalamah [Accessed 30 June 2017].

Bakshi, K., 2013. *Considerations for Software Defined Networking (SDN).* MT, USA, IEEE.

Cisco Networking Academy, 2014. *Connecting Networks Companion Guide.* 1st ed. Indiana: Cisco Press.

Cisco Networking Academy, 2016. *IPSec components and Operations,* San Francisco: Cisco Systems Inc.

Diego Kreutz, F. M. V. R. P. E. V., 2014. Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE,* 103(1), pp. 14-76.

Diego Ongaro, J. O., 2014. *In Search of an Understandable Consensus Algorithm.*
Philadelphia, USENIX.

Fetia Bannour, S. S. A. M., 2017. *A Self-Adaptive Consistency Model for Distributed SDN Controllers.* Le Croisic, RESCOM 2017 Summer school.

Jun-Huy Lam, S.-G. L. H.-J. L., 2015. *Securing distributed SDN with IBC.* Sapporo, IEEE.
Karamjeet Kaur, J. S. N. S. G., 2014. *Mininet as Software Defined Networking Testing Platform* , Ferozepur: Shaheed Bhagat Singh State Technical Campus.

Kevin Phemius, M. B. J. L., 2014. *DISCO: Distributed multi-domain SDN controllers.*
Krakow, IEEE.

Manar Jammal, T. S. A. S. R. A. Y. L., 2014. Software defined networking: State of the art and research challenges. *Computer Networks,* Volume 72, pp. 74-98.

Mehiar Dabbagh, B. H. M. G., 2015. Softwaredefined networking security: pros and cons. *IEEE Communications Magazine,* 53(6), pp. 73-79. Ongaro, D., 2014. *Consensus: Bridging theory and practice,* Stanford: Stanford University. Open Networking Foundation, 2013. *SDN Architecture Overview.* 1st ed. s.l.:Open Networking Foundation.

Santanu Santra, P. P. A., 2013. A Study And Analysis on Computer Network Topology For Data Communication. *International Journal of Emerging Technology and Advanced Engineering,* 3(1), pp. 522-525.

Scott-Hayward, S., 2015. *Design and deployment of secure, robust, and resilient SDN controllers.* London, IEEE.

SDNCentral, LLC, 2017. *Sdxcentral.* [Online] Available at: https://www.sdxcentral.com/sdn/definitions/nort h-bound-interfaces-api/ [Accessed 30 May 2017].

Tianzhu Zhang, P. G. A. B. S. D. D., 2017. The role of the inter-controller consensus in the placement of distributed SDN controllers. *Computer Communications,* 113(2), pp. 1-13.
WestNet Learning, 2003. *Network Design,* Arvada: WestNet Learning.