ISSN 2278-3091
Volume 8, No.1.4, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse2881.42019.pdf
https://doi.org/10.30534/ijatcse/2019/2881.42019

CNDS-SYN Flood Prevention Using Distributed Firewall in Software-Defined WAN Architecture

Bambang Wahyuaji[1], Kalamullah Ramli[2]
[1]University of Indonesia, Indonesia, bambang.wahyuaji@ui.ac.id
[2]University of Indonesia, Indonesia, kalamullah.ramli@ui.ac.id

ABSTRACT

SD-WAN adopts the SDN concept in the WAN area, which provides a dynamic WAN selection to route applications over the best virtual path. In this paper, a case of SD-WAN deployment in a company with a headquarters (data center) and 39 branch offices with redundant WAN MPLS connections is examined. It was expressed that the SYN flood has become a major problem in the company's traditional WAN. The SD-WAN architecture equipped with a virtual distributed firewall was implemented to overcome this problem. The firewall was configured at the company headquarters and pushed to all branch offices. The measurement results indicate that the implementation of the distributed firewall decreases the SYN flood from mitigated subnet to zero percent, while it maintains network latency and throughput. From an economic perspective, the company will reduce its operational expenditure by 63.77 percent for the next five years by deploying the SD-WAN architecture.

Key words : distributed firewall, SD-WAN, SDN, SYN flood, WAN MPLS

1. INTRODUCTION

SD-WAN stands for Software-Defined Wide Area Network, a technology based on Software-Defined Networking (SDN), which is specifically applied in the WAN area and offers virtualization and cost-effective network services. Since its introduction in 2014 (Banks, 2014), SD-WAN has not been growing fast in Indonesia. Expensive MPLS bandwidth, poor internet connectivity quality, and increasing business costs are some reasons that not many institutions or companies have adopted SD-WAN technology in this country (Au, 2016).

A solution of the SD-WAN with a distributed firewall was designed and implemented to prevent the SYN flood in the WAN area of an oil and gas company in Indonesia. This company has 113,613.90 km2 of working area spread across the country and consists of a headquarters, 39 branch offices (five asset offices, 22 field offices, 12 small offices), and thousands of production facilities. The headquarters and branch offices are connected by two redundant providers' WAN MPLS. The measurement results showed that the solution effectively suppresses the SYN flood issue while maintaining network performance.

This paper is organized as follows. Section 1 contains the introduction of the paper, Section 2 discusses the literature review and related research, Section 3 explains the design and implementation of SD-WAN, and Section 4 presents the results and discussion.

2. LITERATURE REVIEW

G. V. Pena and Yu (2014) performed simulations using OpenFlow and Mininet, and the results showed that the distributed firewall did not cause a significant delay in network performance. Suh et al. (2014) demonstrated the basic configuration of a firewall on SDN and the benefits of its usage. Kaur et al. (2015) provided simple firewall programming on SDNs using POX controllers. Rengaraju et al. (2017) also utilized Mininet, OpenFlow, and POX to simulate firewall and an Intrusion Prevention System. Morzhov et al. (2018) stated that the design of the firewall at SDN must follow specific rules so that collisions do not occur. Zope et al.'s (2016) simulations showed that SDN can replace physical network devices with the virtual ones and can also support the development of a firewall and load balancing using Mininet and OpenVSwitch simulations. Kandoi and Antikainen (2015) examined the timeout value of a flow rule and the control plane bandwidth related to DoS attacks. Navid et al. (2017) used real-time network monitoring with sFlow as a visibility protocol to fight DoS attacks.

Lan et al. (2018) presented a dynamic and adaptive load balancing mechanism based on a hierarchical control plane for distributed controllers in SDN using Mininet and Floodlight. The proposed strategy can balance the load of the control plane dynamically and can increase the throughput of distributed controllers. Garrich et al.'s (2019) research covered open source optimization software initiatives for offline planning and online provisioning and the orchestration of SDN/NFV networks and then focused on the

Net2Plan, a complete open-source network optimization framework, as a network optimization NBI application in addition to SDN controllers.

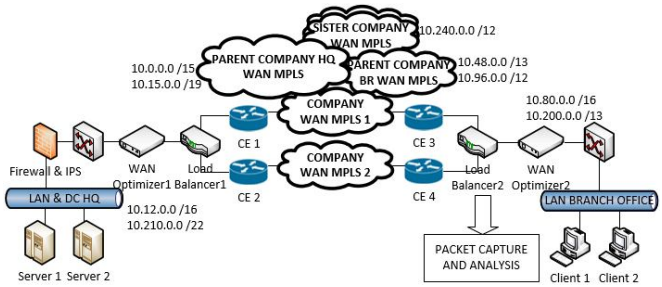


Figure 1: Traditional WAN and SYN flood attack

All these studies demonstrate efforts to activate one of the network services (firewall, load balance, or optimization) with an SDN controller using a simulator. The solution proposed in this paper involves an attempt to combine these services using SD-WAN in an operational WAN area. The scope that limits this research is that the implementation was carried out for a specific company's WAN networks with proprietary devices; the security and performance parameters measured only included distributed firewalls, latency, and throughput, and the solution focuses on preventing SYN flood attacks on a network environment rather than on the source of the attack.

3. DESIGN AND IMPLEMENTATION

Design and implementation were carried out in several stages:

- Reviewing existing architecture, formulating problems, measuring parameters, and specifying requirements.
- Designing new architecture and configurations of SD-WAN
  devices (high-level and low-level design).
- Creating an implementation strategy, scope of works, and time frame for deployment.
- Testing, measuring parameters, and commissioning the results of implementation.

3.1 Traditional WAN Architecture

The company has 40 sites spread across the country, consisting of one headquarters (data center) and 39 branch offices with redundant WAN connections. Figure 1 describes the WAN architecture before the deployment of SD-WAN. The company's headquarters has two IP subnets, which are connected to all branch offices.

Many users in the branch offices reported poor network experiences. The TCP packets in branch offices were captured using the following tcpdump commands:

- *tcpdump -vnni 0.0:nnnp -s0 -c [packet_size] -w /[path]/[file_name].pcap*
  = capturing packets in all ethernet interfaces and ports
- *tcpdump -vnni 0.0:nnnp port 445 -s0 -c [packet_size] -w /[path]/[file_name].pcap*
  = capturing packets in all ethernet interfaces but limited on port 445 only

Tcpdump output files were then analyzed using this Wireshark's filter:

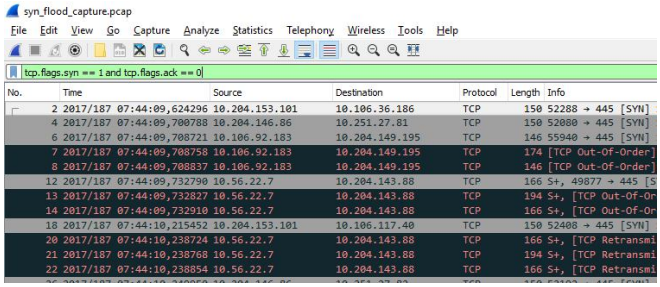


Figure 2: Packets with SYN flood attack

- *tcp.flags.syn == 1 and tcp.flags.ack == 0*
  = displaying only TCP connections that contain a SYN packet

The packet analysis in Figure 2 shows that many SYN flood packets arrived on port 445 and came from parent and sister companies' IP subnets that were connected through the WAN MPLS network.

3.2 The Proposed SD-WAN Architecture

Figure 3 shows the SD-WAN architecture implementation at the company. SD-WAN devices are distributed at all 40 sites. One device is provided as a Master Control Node (MCN) at the headquarters, and 39 other devices are provided as clients at the branch offices. MCN is the central SD-WAN appliance that acts as the master controller of the dynamic virtual WAN (virtual path, QoS, load balancer, WAN optimizer, distributed firewall) and the central administration point for the client nodes. All configuration activities as well as the preparation of the appliance packages and their distribution to clients are performed on the MCN. MCN can monitor the entire virtual WAN, whereas client nodes can monitor only their local Intranets. All sites are connected via redundant MPLS networks, which are managed by two different providers. SD-WAN provides dynamic MPLS selection to route applications over the best virtual path. Each branch office has only one physical device, which contains a logical load balancer, a WAN optimizer, and firewall services. The headquarters location has redundant physical devices to increase availability.

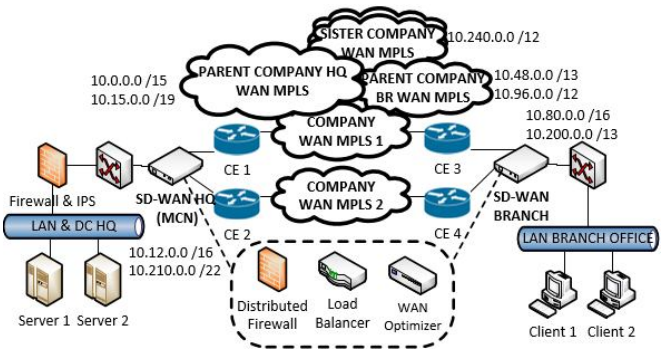


Figure 3: SD-WAN architecture with a distributed firewall

Table 1: Delivery time of SD-WAN and other services

time / services	deployment & installation (days)	total time (days)	saving
SD-WAN	90	90	63.41 %
load balancer	60	246	-
WAN optimizer	99		-
firewall	87		-

It can be observed that SD-WAN devices eliminate the physical devices of the load balancer, WAN optimizer, and firewall. SD-WAN utilizes Network Function Virtualization technology, which simplifies the process to expand and to integrate other network services. The deployment and installation of SD-WAN ran under one project and saved time by around 63.41% compared to traditional WAN, which was separated into three projects, as shown in Table 1.

The SD-WAN implementation strategy must be executed carefully in this sequence: IP addressing, switchover, routing, virtual path (secured with Windows domain integration and SSL authentication), QoS (Quality of Service), WAN optimization, and distributed firewall. The SD-WAN builds an environment ready to support Communication Network and Distributed Systems (CNDS). Distributed computing is widely used at this company, mostly in GGR (Geophysics, Geology, Reservoir) software.

3.3 SD-WAN Distributed Firewall

Distributed firewall policies are created at the global configuration level that can be applied to all sites within the SD-WAN network. Firewall capabilities include defining filter policies of traffic flows, applying global policy templates, and supporting Network Address Translation (NAT), Port Address Translation (PAT), and port-forwarding. Firewall policy (rule) provides the ability to allow, deny, or reject specific traffic flows. Maintaining a clean set of firewall policies is one of the most important factors in firewall operation. Applying these policies individually to each site would be difficult as the SD-WAN network grows. To resolve this issue, groups of firewall filters can be created and applied to all zones or only to specific zones.

The policy attributes used in this implementation include: allow (permit the flow through the firewall), drop (deny the flow through the firewall by dropping the packets), reject (deny the flow through the firewall and send a protocol specific response), IP protocol, source IP address, source port, destination IP address, and destination port.

Stateless firewall policies have been configured to provide protection against the SYN flood on TCP port 445, as shown in Table 2:

- Policies must be free from collisions, as shown by Morzhov et al. (2018).
- Policies number 1 to number 32 denote legitimate

Table 2: Firewall Policies

policy	source		destination		action	from	to
	ip address	port	ip address	port			
1	10.12.0.0 /16	any	10.12.0.0 /16	445	allow	hq	hq
2	10.12.0.0 /16	any	10.80.0.0 /16	445	allow	hq	branch
3	10.12.0.0 /16	any	10.200.0.0 /13	445	allow	hq	branch
4	10.12.0.0 /16	any	10.210.0.0 /22	445	allow	hq	hq
5	10.12.0.0 /16	any	10.0.0.0 /15	445	allow	hq	parent
6	10.12.0.0 /16	any	10.15.0.0 /19	445	allow	hq	parent
7	10.80.0.0 /16	any	10.12.0.0 /16	445	allow	branch	hq
8	10.80.0.0 /16	any	10.80.0.0 /16	445	allow	branch	branch
9	10.80.0.0 /16	any	10.200.0.0 /13	445	allow	branch	branch
10	10.80.0.0 /16	any	10.210.0.0 /22	445	allow	branch	hq
11	10.80.0.0 /16	any	10.0.0.0 /15	445	allow	branch	parent
12	10.80.0.0 /16	any	10.15.0.0 /19	445	allow	branch	parent
13	10.200.0.0 /13	any	10.12.0.0 /16	445	allow	branch	hq
14	10.200.0.0 /13	any	10.80.0.0 /16	445	allow	branch	branch
15	10.200.0.0 /13	any	10.200.0.0 /13	445	allow	branch	branch
16	10.200.0.0 /13	any	10.210.0.0 /22	445	allow	branch	hq
17	10.200.0.0 /13	any	10.0.0.0 /15	445	allow	branch	parent
18	10.200.0.0 /13	any	10.15.0.0 /19	445	allow	branch	parent
19	10.210.0.0 /22	any	10.12.0.0 /16	445	allow	hq	hq
20	10.210.0.0 /22	any	10.80.0.0 /16	445	allow	hq	branch
21	10.210.0.0 /22	any	10.200.0.0 /13	445	allow	hq	branch
22	10.210.0.0 /22	any	10.210.0.0 /22	445	allow	hq	hq
23	10.210.0.0 /22	any	10.0.0.0 /15	445	allow	hq	parent
24	10.210.0.0 /22	any	10.15.0.0 /19	445	allow	hq	parent
25	10.0.0.0 /15	any	10.12.0.0 /16	445	allow	parent	hq
26	10.0.0.0 /15	any	10.80.0.0 /16	445	allow	parent	branch
27	10.0.0.0 /15	any	10.200.0.0 /13	445	allow	parent	branch
28	10.0.0.0 /15	any	10.210.0.0 /22	445	allow	parent	hq
29	10.15.0.0 /19	any	10.15.0.0 /19	445	allow	parent	parent
30	10.15.0.0 /19	any	10.12.0.0 /16	445	allow	parent	hq
31	10.15.0.0 /19	any	10.80.0.0 /16	445	allow	parent	branch
32	10.15.0.0 /19	any	10.200.0.0 /13	445	allow	parent	branch
33	any	any	any	445	reject	all	all

connections between the company's subnets and its parent and sister companies' subnets.

- This firewall does not adopt the principle of "implicit deny all," which means the default action for traffic flow is "allow." Therefore, policy number 33 was created to reject all traffic to TCP port 445.

4. RESULTS AND DISCUSSION

The measurement procedures were performed before and after SD-WAN implementation:

a. Capturing TCP packets in the load balancer (before), capturing TCP packets in the SD-WAN device, and accessing the SD-WAN log (after).
Tools: PuTTY, Tcpdump, Wireshark, SD-WAN device, and Linux

b. Measuring link latency between the host at headquarters and
the host at branch offices.
Tools: Ping, Ms. Windows, and Ms. Excel

c. Measuring link throughput between the host at headquarters
and the host at branch offices.
Tools: Remote desktop, Iperf, Ms. Windows, and Ms. Excel

Table 3: Service cost of SD-WAN and other services

cost / services	managed service cost (IDR)			total cost (IDR)	saving
	per month	per year	5 years		
SD-WAN	196,895,114	2,362,741,364	11,813,706,822	11,813,706,822	63.77%
load balancer	165,676,398	1,988,116,776	9,940,583,880	32,609,526,596	-
WAN optimizer	324,039,442	3,888,473,309	19,442,366,547		-
firewall	53,776,269	645,315,234	3,226,576,169		-

d. Comparing delivery time and service cost between the SD-WAN project and traditional WAN projects for economic consideration.

4.1 Firewall Applied Policies Result

By analyzing SD-WAN log files, TCP packets with destination to port 445 can be checked as shown in Figure 4.

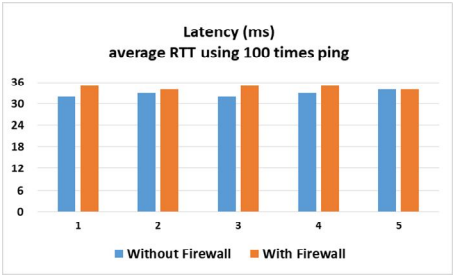
- IP address 10.255.2.244 is accessing port 445 IP address 10.12.3.222: this connection is not listed in “allow” policies no.1–32 → this connection is rejected by policy no.33.
- IP address 10.56.107.14 is accessing port 445 IP address 10.12.20.49: this connection is not listed in “allow” policies no.1–32 → this connection is rejected by policy no.33.
- IP address 10.53.1.19 is accessing port 445 IP address 10.12.3.222: this connection is not listed in “allow” policies no. 1–32 → this connection is rejected by policy no.33.

These results indicate that the firewall has successfully filtered the SYN flood traffic.

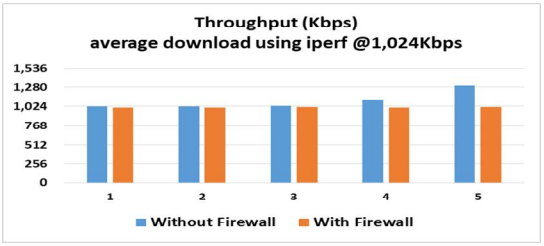
TCP	10.255.2.244	35524	Intranet	TelkomdanXL	10.12.3.222	445	O_DENIED
TCP	10.56.107.14	49658	Intranet	TelkomdanXL	10.12.20.49	445	O_DENIED
TCP	10.53.1.19	36819	Intranet	TelkomdanXL	10.12.3.222	445	O_DENIED
TCP	10.107.56.111	54160	Intranet	TelkomdanXL	10.12.117.12	445	O_DENIED
TCP	10.255.1.80	9951	Intranet	TelkomdanXL	10.12.3.221	445	O_DENIED

Figure 4: Denied SYN flood packets

4.2 Latency and Throughput



(a) Latency



(b) Throughput

Figure 5: Distributed firewall latency and throughput

Latency and throughput measurements indicate that the implementation of the distributed firewall does not have a significant impact on the WAN connection performance. According to Figure 5, the distributed firewall increases the latency value by approximately 5.49% from the initial value and also decreases throughput by around 8.29%. The small impacts on WAN latency and throughput do not disturb the

operational services, which are boosted by an excellent virtual path and QoS performance. End devices, such as a PC, server, storage, and printer, operate normally. All type of applications work well and are stable, including low priority apps, such as email and portals, and high priority apps, such as video conferences, SAP, and GGR software.

5. CONCLUSION

The implementation of the SD-WAN with a distributed firewall has some advantages, i.e., better security, good performance, faster deployment, and lower cost. The firewall works well in preventing SYN floods and increasing network security; however, the firewall causes slight changes on WAN performance, increasing 5.49% latency and decreasing 8.29% throughput. It does not affect the devices and applications' performances. Delivery time is about 63.41% faster because it combines some previous works into one project. It is also economical, reducing operational expenditures by 68.05% for the next five years.

5.1 Future Works

Due to the flexibility of SD-WAN as a distributed system in a virtualization environment, this implementation can be further developed by integrating a stateful firewall or Intrusion Prevention System to improve the accuracy and agility of the SD-WAN security aspects.

ACKNOWLEDGEMENT

Publication of this research is funded by PITTA B grant of University of Indonesia (contract number: NKB-0746/UN2.R3.1/HKP.05.00/2019).

REFERENCES

1. J. G. V. Pena and W.E. Yu**. Development of Distributed Firewall Using Software Defined Networking Technology,** *IEEE International Conference on Information Science and Technology*, Vol. 4, pp. 449-452, April 2014.
2. M. Suh, S. H. Park, B. Lee, and S. Yang. **Building Firewall over the Software-Defined Network Controller,** *IEEE International Conference on Advanced Communications Technology*, Vol 16, pp. 744-748, February 2014. https://doi.org/10.1109/ICACT.2014.6779061
3. K. Kaur, K. Kumar, J. Singh, and N.S. Ghumman. **Programmable Firewall Using Software Defined Networking,** *IEEE International Conference on Computing for Sustainable Global Development (INDIACom)*, Vol 2, pp. 2125-2129, March 2015.
4. P. Rengaraju, V. R. Ramanan, and C. Lung. **Detection and Prevention of DoS Attacks in Software-Defined Cloud Networks,** *IEEE Conference on Dependable and Secure Computing*, pp. 217-223, August 2017. https://doi.org/10.1109/DESEC.2017.8073810
5. S. Morzhov, V. Sokolov, M. Nikitinskiy and D. Chaly. **Building a Security Policy Tree for SDN Controllers**, *2018 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC)*, pp. 1-6, October 2018. https://doi.org/10.1109/MoNeTeC.2018.8572176
6. N. Zope, S. Pawar and Z. Saquib. **Firewall and load balancing as an application of SDN,** *Conference on Advances in Signal Processing (CASP)*, pp. 354-359, June 2016. https://doi.org/10.1109/CASP.2016.7746195
7. R. Kandoi and M. Antikainen**. Denial-of-service attacks in OpenFlow SDN networks,** *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 1322-1326, May 2015. https://doi.org/10.1109/INM.2015.7140489
8. W. Navid and M. N. M. Bhutta. **Detection and mitigation of Denial of Service (DoS) attacks using performance aware Software Defined Networking (SDN),** *2017 International Conference on Information and Communication Technologies (ICICT),* pp. 47-57, December 2017. https://doi.org/10.1109/ICICT.2017.8320164
9. W. Lan, F. Li, X. Liu and Y. Qiu. **A Dynamic Load Balancing Mechanism for Distributed Controllers in Software-Defined Networking,** *2018 10th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, pp. 259-262, February 2018. https://doi.org/10.1109/ICMTMA.2018.00069
10. M. Garrich, F. Moreno-Muro, M. Bueno Delgado and P. Pavón Mariño. **Open-Source Network Optimization Software in the Open SDN/NFV Transport Ecosystem**, *Journal of Lightwave Technology*, vol. 37, no. 1, pp. 75-88, Jan 1, 2019. https://doi.org/10.1109/JLT.2018.2869242
11. E. Banks, **Software-Defined WAN: A Primer,** The Network Computing, 2014, Available at https://www.networkcomputing.com/networking/software-defined-wan-primer
12. G. Au, **How to Get Started with SD-WAN: An Asia Pacific Focus,** 2016, available at https://www.slideshare.net/GinnyAu/how-to-get-started-with-sdwan-an-asia-pacific-focus