Abstract

Software Defined Networking (SDN) is a new trend in networking. SDN replaces traditional networking by separating control plane and data plane. SDN is managed by centralized controller. SDN has certain challenges such as security, reliability, controller failover, load balancing, traffic engineering. Security in SDN is more challenging than traditional networking. One of the security challenges in networking is DoS (Denial of Service) attack which can be created using various mechanisms. This paper review different DoS attacks which can be possible on control plane and data plane. This paper have surveyed, studied and identified the security challenges and different existing techniques to mitigate Dos attacks in SDN. Future researches on DoS attack mitigation techniques are indicated in this paper.

References

1. Rajat Kandoi, Markku Antikainen “Denial-of-Service Attacks in OpenFlow SDN”, IFIP
2015.

2. Software-Defined Networking (SDN) Definition
https://www.opennetworking.org/sdn-resources/sdn-definition

3. The Open Networking Foundation (ONF)
https://www.opennetworking.org/about/onf-overview


5. Floodlight Is an Open SDN Controller http://www.projectfloodlight.org/floodlight/

6. Production Quality, Multilayer Open Virtual Switch http://openvswitch.org/


8. Understanding the SDN Architecture
https://www.sdxcentral.com/sdn/definitions/inside-sdn-architecture


17. “Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis”. The SANS Institute, 2011.

18. S. Shin, V. Yegneswaran, P. Porras, and M. Tyson, “Fresco: Modular composable security services for software defined network In NDSS",2013


Index Terms

Computer Science

Security
Keywords

Software Defined Network (SDN), Open Flow, security, DoS, ONF (Open Networking Foundation), TCP-SYN, ICMP, Southbound interface (SBI), Northbound interface (NBI).