Network Security for SDN

Introduction

The new network based on software-defined Network SDN and network function virtualization NFV will replace the traditional network, so it is urgent to study the network security architecture based on the new network environment. This paper presents a software - defined Security SDS architecture [1].
The plane separation technology introduces many new loopholes in the SDN data plane. In order to facilitate taking proactive measures to reduce the damage degree of network security events, this paper proposes a security situation prediction method based on particle swarm optimization algorithm and long-short-term memory neural network for network security events on the SDN data plane [2].

Problem statement

- It can realize the deployment , arrangement and customization of virtual security function VSFs.
- It implements fine-grained data flow control and security policy management.
- Analyzes the different types of attacks that different parts of the system are vulnerable to.
- The defender can disable the network attacks by changing the server-side security configuration scheme.

Literature Review

In the network security situation assessment, a parallel reduction algorithm based on attribute importance matrix is proposed to reduce the attributes of the data source data. A network security situation assessment model based on a gravity search algorithm is proposed to optimize support vector machines to reduce the error between the evaluation value and the actual network security situation value [1].

In the network security situation prediction, a network attack prediction model combining extreme value   which is effective for both long term and short term prediction [2]

Methodology

The design idea of NFV is to use the general x86architecture machine to replace the underlying heterogeneous special equipment's.
The devices are open and compatible. Then using virtualization technology, the device control plane is running on the server, which provides different functions in the virtual layer and allowing functions to be combined and separated.
SDN logical layers ： Application layer ,control layer and infrastructure layer
Network devices : switches , routers , etc.
Security tools :

- Firewall
- Intrusion detection
- Intrusion prevention

Outcomes

Centralized control and network programmability

Global network view and traffic analysis

Can be done for collect, detect, protect.

References

[1] Lina, Z. and Dongzhao, Z., 2020, March. A New Network Security Architecture Based on SDN/NFV Technology. In 2020 International Conference on Computer Engineering and Application (ICCEA) (pp. 669-675). IEEE.

[2]   Sheng, M., Liu, H., Yang, X., Wang, W., Huang, J. and Wang, B., 2020, August. Network Security Situation Prediction in Software Defined Networking Data Plane. In 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA) (pp. 475-479). IEEE.