International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 4, April - 2014

Software Defined Network Based threat Defence Security Model

Parthiban A
Department of Information Security and Cyber Forensics
SRM University
Chennai, India

Godwin Ponsam J
Department of Information Security and Cyber Forensics
SRM University
Chennai, India

***Abstract*— It is generally considered as a challenge to provide network security to our network. We require various device such as firewalls, intrusion detection and prevention systems. These network security devices must be constantly monitored and managed by security operation center [10]. The logs and alerts by various devices has to be analyzed and remedial action must be taken at real time, hence manual analyst is required to inspect the logs and alerts. This method has considerable time lag which might lead to network outbreak at some emergency situation. In this paper we propose dynamic blocking of critical anomalous traffic using software defined networking [1] infrastructure. We have adopted OpenFlow protocol [2] to provide communication between controller and OpenFlow-hybrid switch. Controller [1] runs applications such as intrusion detection system [3] and rule database. Security information and event management collects all these logs and alerts from network security devices. When a critical incident is triggered, it is sent to the controller to block critical anomalous traffic immediately.**

Keywords- Intrusion detection system, OpenFlow, Flow table, OpenFlow channel, software defined networking.

I. INTRODUCTION

Network security now a days has become indispensable for everyone. Securing our network from various known and unknown attack is a challenging task. Attacks from both internal and external network are threat to information security. Security professionals are necessary to analyze the various network happening and identify major threat to our network. Various security mechanism has to be deployed to detect and prevent intrusions of our network. Whenever a new technology emerges security professionals are in the position to look for security in it. In this paper, the whole idea is about using Software Defined Networking technology for providing security to our network.

II. INTRUSION DETECTION SYSTEM

Network-based intrusion detection system is a powerful tool to elevate security level of networks. A network-based ID system monitors the traffic on its network segment for harmful data. It is used to prevent various attacks in future. This is generally possible by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment. Network-based IDS has some sensors looking at the packets which pass through it. These sensors are capable of only analyzing the packets that occur to be carried onto the network segment it is attached to. Packets are considered to be of interest if they match a signature which resides on database.

A. Intrusion detection operation modes

- On-path detection

The IDS is placed on the packet transverse route, so the traffic which goes on that path will be analyzed for malicious data before being forwarded to the device. As it is placed on the path of a route it affects the performance of network

- Off-path detection

In this approach IDS is a separate node which is connected to a network switch. Every packet on the network is mirrored and sent to the IDS for inspecting traffic to detect network intrusions. Unlike on-path detection this approach will not affect the performance of network. In this paper we use this approach for the deployment of IDS to detect the malicious data on the network. Hence performance of network can be greatly increased.

III. SOFTWARE DEFINED NETWORKING

A new paradigm in networking, software defined networking (SDN), advocates separating the data plane and the control plane, making network switches in the data plane simple packet forwarding devices and leaving a logically centralized software program to control the behavior of the

entire network [1]. SDN announces new opportunities for network management and configuration methods. The controller acts as an intelligent module to dictate the behavior of the network. Despite switching and routing capabilities, controller can also act as an interface for running various applications. These applications facilitate the management capabilities which are specified in the layers of SDN as shown in Figure 1.

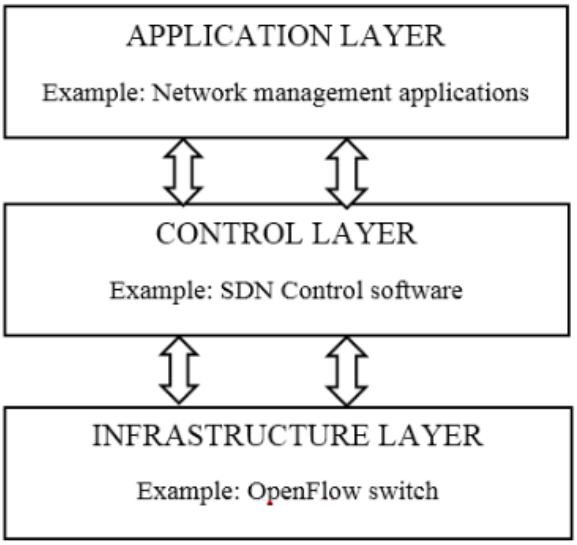

Figure 1. Layers of SDN

IV. OPENFLOW NETWORK

OpenFlow is an open standard that allows researchers to run experimental protocols in the SDN infrastructure. The OpenFlow Switch [2] and Controller communicate via the OpenFlow protocol, which defines messages, such as packet-received, send-packet-out, modify-forwarding-table, and get-stats. It enables one controller to manage all OpenFlow switches remotely. The main component OpenFlow network consists of the following,

A. OpenFlow switch

An OpenFlow Switch consists of one or more tables and a group table, which performs packet lookups, forwarding and an OpenFlow channel [2] to the external controller (Figure 3). The switch communicates with the controller and the controller manages the switch via the OpenFlow protocol.

Types of OpenFlow switch

- OpenFlow-only switch

The OpenFlow switches supports only OpenFlow operation. In such switches, all the packets are processed by OpenFlow pipelines, and cannot be processed otherwise.

- OpenFlow-hybrid switch

The OpenFlow switches support both OpenFlow operation and normal operation such as switching, routing, ACL and QOS in traditional network [2].

B. Flow table

OpenFlow switch contains number of flow table [2] which are used to process the packet. When handled by a flow table, the packets are matched against the flow entries of the flow table to select a flow entry. If a flow entry is found, the instruction set included in that flow entry is executed. These instructions may send the packet to another flow table, where the same process is repeated again. If the packet doesn't match with any flow entries, by default unmatched packet is dropped (discarded) but we override this default and specify another behavior to process the packet on table miss. This flow table entries is populated by the controller. Main components of a flow entry in a flow table shown in Table 1.

Table 1. Main components of a flow entry in a flow table

Match fields	Priority	Counter	Instructions	Timeouts	Cookies

Each flow table entry contains:

- Match fields: To match against packets. This field consists of the ingress port packet headers and optional metadata specified by a previous table.
- Priority: Matching parameter of the flow entry.
- Counters: Updated when packets are matched.
- Instructions: To modify the action set or pipeline processing.
- Timeouts: Maximum amount of time that flow entry exist in the flow table.
- Cookie: Opaque data value chosen by the controller. May be used by the controller to filter flow statistics, flow modification and flow deletion. Not used when the packets are processed.

C. OpenFlow channel

OpenFlow channel [2] is an interface through which the data is transferred between OpenFlow switch and controller. It should be a secure channel to prevent the man in the middle attack.

D. OpenFlow protocol

The OpenFlow protocol provides an open and standard way for controller to communicate with an OpenFlow switch. Using the OpenFlow protocol, the controller can update, add and delete flow entries in the flow tables, both reactively (in response to packets) and proactively. OpenFlow specification [2] provides excellent

source of information about OpenFlow protocol and its usage. The scope of OpenFlow switch specification is shown in Figure 2.

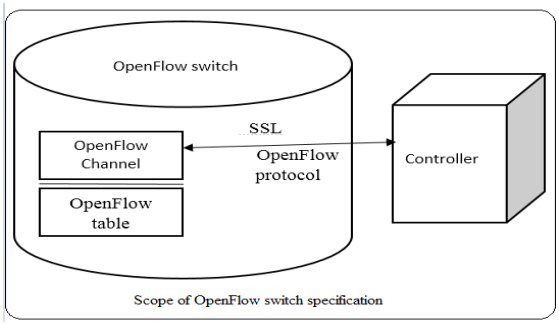

Figure 2. Scope of OpenFlow switch specification

E. OpenFlow pipeline

The OpenFlow pipeline [2] of every OpenFlow switch encompasses multiple flow tables, each flow table containing multiple flow entries. The OpenFlow pipeline processing defines how packets interact with those flow tables. An OpenFlow switch should have at least one flow table and can optionally have more than one flow table. An OpenFlow switch with only a single flow table is valid, in this case pipeline processing is greatly reduced. Using pipeline, instruction packets are directed to the other flow table.

V.METHODOLOGY

In recent days many research has been in progress to make OpenFlow switch perform efficient switching and routing using software defined network. In this paper we use hybrid OpenFlow switch which has two tables, first one is access control flow table which is used to only block the critical traffic of our network and another is normal content addressable memory table which is used for L2 switching.

A. Access Control flow table

Access control flow table is used to block the malicious packet before being forwarded for normal switching. This table blocks the traffic with some matching conditions which is placed as access control flow entries which shown fig 4. This table simply acts as a firewall to block the critical traffic using flow entries. This is shown in Table 2.

Table 2. Access control flow table with sample entry

Rule id	Priority	Ingress port	MAC source address	MAC destination address
1234	1	2	*(any)	*(any)
IP source address	IP destination address	TCP source port	IP destination address	Action
6.6.6.6	*(any)	*(any)	3389	DROP

In Table 2. Access control flow entry checks for any packet which has source IP address 6.6.6.6 trying to connect with destination machine on 3389 port. If the criteria specified by the access control flow table matches with the specified criteria the packet is dropped. These entries are generally populated by the controller using OpenFlow protocol.

B. Content Addressable Memory table

Primarily when packet is entering the switch, it has to be processed by access control flow table. If the packet doesn't match with any entries in access control flow table then it will be forwarded to the CAM [9] table for normal L2 switching. Pipeline instructions are used to control the flow between access control flow table and CAM table.

C. IDS

Controller has various applications which run on in it, one such application is IDS. Every packet entering into switch will be mirrored and sent to the IDS to detect the malicious data on the network. Basically IDS will detect intrusions in two ways; one is Signature-based IDS which checks the database of previous attack signatures and known system vulnerabilities. The meaning of word signature is a recorded indication of an intrusion or an attack. Each intrusion leaves a footprint behind (e.g., data packets nature, attempt failed to run an application, failed logins, folder and file access etc.), these footprints are called signatures and can be used to recognize and prevent the same attacks in the future. Another one is Anomaly-based Intrusion which is used to identify active Intrusion Detection Systems (IDS) using references as a baseline or using the learned pattern of normal system activity. Deviations from this baseline or pattern trigger an alarm. The alerts generated by the IDS sent to the security information and event management [8] (SIEM).security information and management is responsible for event management and incident generation.

D. Security Information and Event Management

Security information and event management (SIEM) is a method of security management that provides a complete view of an organizations information technology (IT) security. SIEM systems collect security associated events from end user devices, servers, network devices and even specialized security devices like antivirus firewalls or intrusion prevention systems. This system is mainly used to create an incident from collected security event using some pre-defined rule. From SIEM critical incident will be sent to the rule database. Other critical incidents will be sent to the SOC (security operation center).

E. Rule database

The rule database has some pre-defined format to create access control rule which will be populated in access control flow table to block the critical anomalous traffic. Only for critical incidents it will have a rule format. Whenever that critical incident is triggered, the rule database will parse the packet header information and create access control rule

according to the fine-tuned format which are assigned for that particular critical incident. Other incidents will be sent to the security operation center for further analysis.

Example: Bot activity with external source IP address (4.5.5.5) incident – predefined format will be like block any packet with IP address (4.5.5.5) the flow entries of access control looks like Table 3.

Table 3. Sample flow entries for critical incident.

Rule id	Priority	Ingress port	MAC source address	MAC destination address
1111	4	5	*(any)	*(any)
IP source address	IP destination address	TCP source port	IP destination address	Action
4.5.5.5	*(any)	*(any)	*(any)	DROP

As specified in Table 5. With the combination of different address and port we can block critical traffic successively.

F. Security Operation Center

A SOC is the people, procedures and technologies involved in creating situational awareness through detection, containment, and remediation of IT threats. A SOC manages incidents for the enterprise, ensuring that they are properly identified, analyzed, communicated, actioned/defended, investigated and reported. The SOC holds analysts who analyses the incidents and comes up with remedial action.

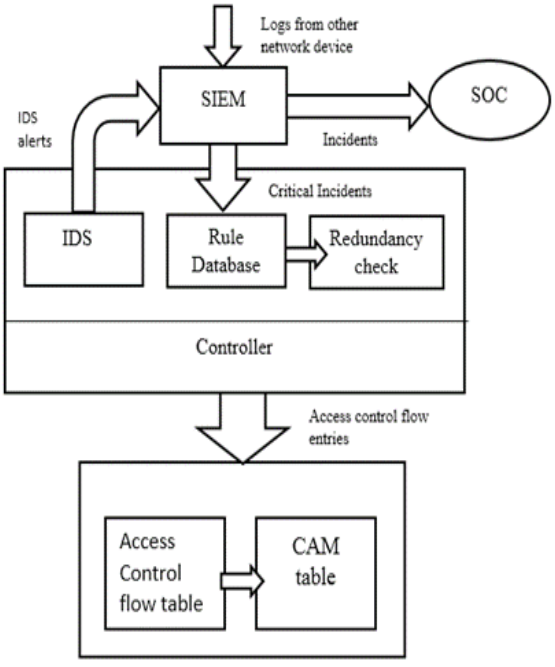

Figure 3.Architecture diagram

G. Redundancy check

Once the rule is generated from the rule database it will send that rule to redundancy check module. Module has to be completely updated with access control flow entries information. Before forwarding the access control flow entries to controller, it is checked for the particular rule which might have been already implemented. If it is a new rule then it will be forwarded to the controller. The controller will then update the access control flow table with the current rule it has. Overall architecture of our proposal is shown in the Figure 3.

H. Proposed Pseudo code

Step 1: Whenever the packet is coming inside the OpenFlow switch, send the mirrored copy of packet to the IDS.

Step 2: Then processes the packet through the access control flow table.

Step 3: If the parsed packet header field matches with the rule then drop the packet.

Step 4: If the packet does not matches with any rule then forward the packet to CAM table for normal L2 switching.

Step 5: When the critical incident from SIEM is triggered send that incident to rule database.

Step 6: If that critical incident has pre-defined rule format, then create a rule by parsing the packet.

Step 7: check whether the rule has already been implemented, if not send it to controller.

Step 8: Update that rule in access control flow table through a centralized controller.

VI. CONCLUSION AND FUTURE WORK

In this paper we have proposed dynamic blocking of critical anomalous traffic which hence prevents the network outbreaks during emergency condition. Before the critical incidents are forwarded to analysis, access control rules are implemented at the device level, this prevents the spreading of malicious traffic in our network. Since the centralized controller also behaves as an IDS, the cost of deploying IDS sensors for capturing packet will be greatly reduced. Future enhancements includes implementation of OpenFlow-only switch with dynamic packet forwarding capability and access control mechanisms.

REFERENCES

[1] Hyojoon Kim and Nick Feamster, Georgia Institute of Technology“Improving Network Management using Software Defined Network “
[2] OpenFlow Switch Specification version: 1.4.0 Available:https://www.opennetworking.org
[3] Stephen Northcutt, Judy Novak “Network Intrusion Detection System
[4] N.McKeown, et. al., "OpenFlow: Enabling Innovation in Campus Networks", SIGCOMM CCR, Vol. 38, Issue 2, march 2008.

[5] Stephen Northcutt, Mark T. Edmead "inside network perimeter security"
[6] www.openflow.org
[7] www.sdncentral.com
[8] http://en.wikipedia.org/wiki/Security_informatio n_and_event_management
[9] http://en.wikipedia.org/wiki/CAM_Table
[10] http://en.wikipedia.org/wiki/Information_security_operations_center
[11] http://en.wikipedia.org/wiki/Computer_security_incident_management
[12] http://www.securityincidents.org/