ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 4, April 2017

A Review of Load Balancing in Network-Wide Intrusion Detection Systems

[1] Miss. Prachi N. Deshmukh, [2]Dr. V. M. Thakare
[1][2]SGBAU, Amravati,Maharashtra, India,

***Abstract*- There are various stakeholders having similar goals as well as policies due to which modification to the present internet is restricted to incremental updates; implementation of every novel fundamentally extraordinary innovation is beside inconceivable. To deal with this issue, proposed the concept of network virtualization, here designed as a diversifying attribute without having restriction of any system. By permitting multiple heterogeneous system structures to live together on a shared physical substrate, network virtualization gives flexibility, promotes diversity, and promises security and increased manageability. It reduces the maximum computation load, provide better resilience under traffic variability, and offer improved detection coverage.**

***Keywords:* intrusion detection, traffic measurement, computer network management, Network virtualization, Security;**

I. INTRODUCTION

A new approach for detecting security attacks on software systems by monitoring the software system performance signatures is introduced [1]. Under conditions of heavy traffic load or sudden traffic bursts, the peak processing throughput of network intrusion detection systems (NIDS) may not be sufficient for inspecting all monitored traffic and the packet capturing subsystem inevitably drops excess arriving packets before delivering them to the NIDS [2]. Network intrusion detection (NIDS) and prevention systems (NIPS) serve a critical role in detecting and dropping malicious or unwanted network traffic. These have been traditionally deployed as perimeter defense solutions at the boundary between a trusted internal network and the untrusted Internet [3]. As traffic volumes and the types of analysis grow, network intrusion detection systems (NIDS) face a continuous scaling challenge. Management realities, however, limit NIDS hardware upgrades to occur typically once every 3-5 years. Given that traffic patterns can change dramatically, this leaves a significant scaling challenge in the interim [4]. Denials of Service (DoS) threats are executed to make a network service unavailable for legitimate users. The category of Slow DoS attacks (SDA) exploits low amounts of bandwidth to generate anomalies on well known protocols (e.g., HTTP, FTP), thus reducing the number of concurrent connections accepted by the servers or making daemons crash. In this context, various detection methodologies are available, by working either at the application layer or at the network/ transport layers [5].

In this proposed methodology, proposed the concept of network virtualization has designed as a diversifying attribute without having restriction of any system. By permitting multiple heterogeneous system structures to live together on a shared physical substrate, network virtualization gives flexibility, promotes diversity, and promises security and increased manageability. And reduce the maximum computation load, provide better resilience under traffic variability, and offer improved detection coverage. NETSECVISOR, which can utilize existing predeployed (fixed-topology) security devices and leverage software-defined networking technology to, virtualizes network security functions.

II. BACKGROUND

Present architecture for monitoring mission-critical systems for security intrusion that takes advantage of system-wide performance signatures. In addition, the suggest an approach to distinguish between performance signatures that can be identified as being associated with security intrusions and those that are associated with faults that will lead to soft failures [1]. Selective packet discarding is a best effort approach that enables the NIDS to anticipate overload conditions and minimize their impact on attack detection. Instead of letting the packet capturing subsystem randomly drop arriving packets, the NIDS proactively discards packets that are less likely to affect its detection accuracy, and focuses on the traffic at the early stages of each network flow [2]. Explore a different design alternative. Instead of trying to scale processing at a few chokepoints, an approach exploits the existing replication of each packet along its forwarding path. In doing so, the author depart from the single-vantage-point strategy, and permit the different nodes on a packet's forwarding path to be candidates for performing the analysis [3]. Design a general architecture for network-wide NIDS

ISSN (Online) : 2394-6849
International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 4, April 2017

deployment that leverages three scaling opportunities: on-path distribution to split responsibilities, replicating traffic to NIDS clusters, and aggregating intermediate results to split expensive NIDS processing [4]. The method concentrates their attention to the communication level. The method analysis focuses on the quantity of data directed from the transport layer to the application layer. Although analyze data relative to the application layer, payload inspection is not needed [5].

This paper introduces Section I introduction. Section II discusses Background. Section III discusses previous work. Section IV discusses existing methodologies. Section V discusses the attributes and parameters and how these are affected on images. Section VI proposed method and outcome result possible. Finally Section VIII concludes this review paper.

III. PREVIOUS WORK DONE

Alberto Avritzer et al. (2010)[1], present architecture for monitoring mission-critical systems for security intrusion that takes advantage of system-wide performance signatures. In addition, the suggest an approach to distinguish between performance signatures that can be identified as being associated with security intrusions and those that are associated with faults that will lead to soft failures.

Antonis Papadogiannakis et al. (2010)[2], proposed selective packet discarding, a best effort approach that gracefully reduces the amount of traffic that reach the detection engine of the NIDS by selectively discarding packets that are less likely to affect its detection accuracy.

Vyas Sekar et al. (2010)[3], a provided systematic formulations for effectively managing NIDS and NIPS deployments. In doing so, used a network-wide coordinated approach, where different NIDS/NIPS capabilities can be optimally distributed across different network locations depending on the operating constraints – traffic profiles, routing policies, and the resources available at each location.

Heorhiadi et al. (2012)[4], proposed a balancing computation-communication tradeoffs in scaling network-wide intrusion detection systems. And show that the proposal can substantially reduce the maximum computation load, provide better resilience under traffic variability, and offer improved detection coverage.

M. Aiello et al. (2014)[5], proposed a problem of detection of "Slow" Denial of Service attacks. The problem is particularly challenging in virtue of the reduced amount of bandwidth generated by the attacks. A novel detection method is presented, which analyzes specific spectral features of traffic over small time horizons. No packet inspection is required. Extrapolated data refer to real traffic traces, elaborated over the Local Area Network of Institute. Different kinds of attacks have been considered as well.

IV.EXISTING METHODOLOGIES

1] Architecture for security intrusion detection using off-the-shelf security monitoring tools and performance signature

Architecture for monitoring mission-critical systems for security intrusion that takes advantage of system-wide performance signatures. In addition, the suggest an approach to distinguish between performance signatures that can be identified as being associated with security intrusions and those that are associated with faults that will lead to soft failures.

2] Selective packet discarding approach

In selective packet discarding, first discuss which packets should be considered for discarding, and propose a selection based on the position of packets in their flows. Then, describe the performance measurements that the NIDS should perform periodically to monitor the system's load and decide when selective packet discarding should be triggered. Finally, present an algorithm that dynamically estimates how many packets should be dropped according to the system performance measurements.

3] Systematic formulations for effectively managing NIDS and NIPS deployment

Explore a different design alternative. Instead of trying to scale processing at a few chokepoints, an approach exploits the existing replication of each packet along its forwarding path. In doing so, the author depart from the single-vantage-point strategy, and permit the different nodes on a packet's forwarding path to be candidates for performing the analysis.

For NIPS Deployment:

Each rule C_i is associated with three types of resources:(1) CPU processing load 〖CpuReq〗_i per packet, (2) memory load 〖MemReq〗_i if it needs to maintain any per-flow or cross-packet state, and (3) and the TCAM required 〖CamReq〗_i per rule. Note that the 〖CamReq〗_i is per-rule rather than per-packet or per-flow.

4] A general NIDS architecture to leverage three opportunities: offloading processing to other nodes on a packet as routing path, traffic replication to off-path nodes, and aggregation

ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 4, Issue 4, April 2017

This paper proposed a general NIDS architecture to leverage three opportunities: offloading processing to other nodes on a packet as routing path, traffic replication to off-path nodes (e.g., to NIDS clusters), and aggregation to split expensive NIDS tasks. And they implemented a lightweight shim that allows networks to realize these benefits with little to no modification to existing NIDS software. Their results on many real-world topologies show that this architecture reduces the maximum compute load significantly, provides better resilience under traffic variability, and offers improved detection coverage for scenarios needing network-wide views.

5] Online intrusion detection approach

This paper addresses the problem of detection of "Slow" Denial of Service attacks. The problem is particularly challenging in virtue of the reduced amount of bandwidth generated by the attacks. A novel detection method is presented, which analyzes specific spectral features of traffic over small time horizons. No packet inspection is required. Extrapolated data refer to real traffic traces, elaborated over the Local Area Network. Different kinds of attacks have been considered as well.

A. Detection Mechanism:

The chosen feature drives an anomaly-based analysis of web traffic. Anomaly-based detection may be more adaptive than other complicated tools as it simply looks at sudden changes of flows statistics, while providing good detection rates. The author has defined two observation horizons (OHs): the current OH and the previous OH. They are two subsequent temporal periods in which we monitor the chosen feature. More specifically, on both the OHs, we look at the temporal behavior of the feature as a signal over time s(t). If not otherwise stated, the signal is sampled every 1 second. Under a given metric m(.), a difference δ between the signals registered over the two OHs (s0(t) and s-1(t), respectively) is computed: δ=m(s0(t); s-1(t)).

B. Metrics:

Two metrics are considered. The first one is based on the simple average of s(t):

$$\delta^{l,a}_{E\{.\}} = (E[s0(t)] - E[s-1(t)])^2 \quad \ldots\ldots\ldots \quad (1)$$

The aim of the metric is to capture all the situations in which bursts of packets lead to clear indications about a running attack. The second one is the mutual information I(.,.) of the Fast Fourier Transform (FFT) F(.) applied to s0(t) and s-1(t):

V. ANALYSIS AND DISCUSSION

The performance signatures derived from the execution of the security tests. The intrusion detection ability of the off-the-shelf tools composing the security infrastructure is shown [1].

Experimental environment consists of two PCs interconnected through a 10 Gbit switch. The first PC is used for traffic generation, which is achieved by replaying real network traffic traces at different rates using tcpreplay. The traffic generation PC is equipped with an Intel Xeon 2.00 GHz CPU with 6 MB L2 cache, 2 GB RAM, and a 10 Gbit network interface. [2].

Traffic changes: formulate the problem in a static setting. This raises concerns regarding traffic bursts, changing traffic profiles, etc. Routing changes: Network paths are largely stable on the timescales for per-session analysis. However, when route changes do occur and recomputed the optimal solutions, there is a concern that this may affect correctness. Provisioning and Upgrades: And also extend the formulations to describe what-if provisioning scenarios: where should an administrator add more resources or augment existing deployments with more powerful hardware. Aggregated analysis: Certain kinds of analysis need aggregated network-wide views [3].

One concern with distribution is ensuring consistency when configurations are recomputed. And use standard techniques from the distributed systems literature (e.g., two-phase commit). And also use simpler domain-specific solutions; e.g., whenever new configurations are pushed out, the NIDS nodes continue to honor both the previous and new configurations during the transient period. This may potentially duplicate some work, but ensures correctness of operation [4].

The author has executed tests by analyzing the traffic on a web server running the Apache2 daemon. The monitored server offers support to the web site of their Institute. The inherent traffic has been monitored on the local LAN. The server is configured to simultaneously manage at most C = 150 connections and at most Csimultaneous = 100 simultaneous persistent connections. [5].

VI. PROPOSED METHODOLOGIES

Figure1. Shows the system architecture of proposed system a typical operation of

ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 4, April 2017

NETSECVISOR works as follows. A network administrator registers network security devices (both physical devices and virtual appliances) to NETSECVISOR. After registration, cloud tenants need to create their security requests and submit them into NETSECVISOR. Then, NETSECVISOR parses the submitted security requests to understand the intention of tenants and writes the corresponding security policies to policy table. Next, if NETSECVISOR receives a new flow setup request from a network device, it checks whether this flow is matched with any submitted policies. If it is, NETSECVISOR will create a new routing path and corresponding flow rules for the path. At this time, NETSECVISOR guarantees that the routing path includes required security devices that are defined in a matched policy. After this operation, it enforces flow rules to each corresponding network device to forward a network flow. If any of security devices detects malicious connection/content from monitored traffic, it will report this information to NETSECVISOR. Based on the report and submitted policies NETSECVISOR enables a security response function to respond to malicious flows accordingly.

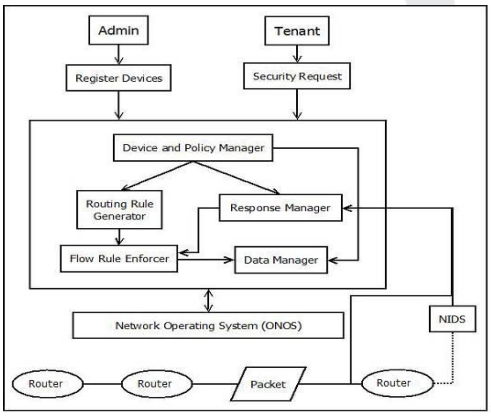

Figure1. System Architecture

OUTCOME AND POSSIBLE RESULT

The results on many real-world topologies show that this architecture reduces the maximum compute load significantly, provides better resilience under traffic variability, and offers improved detection coverage for scenarios needing network-wide views.

VII. CONCLUSION

This paper analyses various techniques used for Network Monitoring and Trust Routing. Also given the advantages and drawbacks present in the different studies performed by various researchers. To deal with drawbacks in present systems and presented an idea of the new system.

FUTURE SCOPE

In future work, the concept of network virtualization is use for deal with the drawbacks of existing system and presents an idea of the new system.

REFERENCES

1] A. Avritzer, R. G. Cole and E. J. Weyuker, "Monitoring for security intrusion using performance signature", in tactical WOSP/SIPW ACM JANUARY 2010, pp.93-103.

2]Antonis Papadogiannakis, Michalis Polychronakis and Evangelos P. Markatos," Improving the accuracy of Network Intrusion Detection Systems Under Load Using Selective Packet Discarding" EUROSEC ACM 2010, pp. 15-21.

3] Sekar, V., Krishnaswamy, R., Gupta, A., and Reiter, "Network-wide deployment of intrusion detection and prevention systems", in proc. CoNEXT '10, 2010.

4] Victor Heorhiadi, Michael K. Reiter, and Vyas Sekar,"New Opportunities for Load Balancing in Network-Wide Intrusion Detection System", in proc. CoNEXT ACM DECEMBER 2012. pp. 361-372.

5] M. Aiello, E. Cambiaso, G. Papaleo, " An On-line Intrusion Detection Approach to Identify Low-Rate DoS Attacks", in proc. IEEE 2014.