A Hybrid Intrusion Detection Architecture for Defense against DDoS Attacks in Cloud Environment

Sanchika Gupta, Susmita Horrow, and Anjali Sardana

E&CE Department
IIT Roorkee
Roorkee, India
sanchigr8@gmail.com, dr.anjalisardana@gmail.com

Abstract. Cloud Computing is emerging out as the future of next generation architecture for information technology enterprises. But due to its popularity, it is vulnerable to various unwanted attacks. One of the solutions is intrusion detection system. The Existing architectures of IDS in cloud environment are deployed on the network periphery of each guest OS that offers high attack resistance at the cost of visibility. In this paper, we propose hybrid architecture for deployment of intrusion detection system which takes into account security at both the front end and the clusters. This Paper also includes a critical review of previously proposed architectures on deployment of Intrusion Detection Systems in Cloud Environment and a detailed description of the research Gaps identified. Our approach leverages VMware virtualization techniques using open nebula as a test bed for deploying our proposed system.

1 Introduction and Literature Review

Cloud Computing provides the means through which computing infrastructure, applications, business processes to personal collaboration can be delivered as a service. These services expose cloud to the risk of security attack. One of the major attacks field is DDoS attacks.

In [1], an IDS system is deployed in each cloud computing region. These IDSs will cooperate with each other by exchanging alerts to reduce the impact of the DoS attack. However vulnerability to attacks is high as there is no central control. [2] Provides a generic model in which each instance of IDS has to monitor only a single user but has no cooperation.

2 Proposed Architecture, Results and Conclusions

We identified that providing full control to the users is risky and Location of deployment of IDS in cloud is a major decision factor for accurate detection and response to attacks An IDS framework for defense against DDoS attacks in cloud is shown in Fig 1, which is hybrid architecture. It consists of Cloud service users (CSU's) and a cloud service provider (CSP). A third party provides authentication to the cloud users.

M. Parashar et al. (Eds.): IC3 2012, CCIS 306, pp. 498–499, 2012.

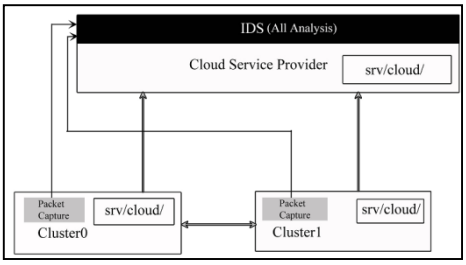

Fig. 1. Hybrid IDS Architecture

Fig. 2. CPU usage at Front end

Each Cluster node and Front-End are connected in mesh topology. The Front-End provides the NAT services. Hence, all the traffic flowing to and coming from the cluster nodes has to traverse the Front End. A single IDS is deployed at the Front End. IDS will be able to see all the traffic related to the virtual hosts in the cloud, and prove a very good point of observation. This IDS alerts, are stored in a common shared file system (NFS). The IDS deployed is Snort [3], it is a signature based NIDS. Attacks are generated using a Distributed- Internet Traffic Generator (D-ITG) [4] and using nmap port scan. The IDS at Front end sniffs the traffic from the Front-End and external traffic moving in and out of the cluster nodes. At each cluster node wire shark capture the traffic in a .pcap file, which is stored in the shared directory. This .pcap file is read by Snort as if packets are directly coming off the wire. Fig. 2 shows us the results of deployment where packets are captured at the Virtual Hosts and analyzed at the Front-End.

In this proposal, various deployment strategies of Snort have been analyzed in an open source cloud computing environment namely Open Nebula. Finally in the proposed architecture, packets are captured at the virtual hosts using wire shark which act as a sensor and later these packets are analyzed at front end. Moreover in the proposed architecture, deployment is done to provide security only for Infrastructure layer using open nebula.

References

1. Lo, C.-C., Huang, C.-C., Ku, J.: A Cooperative Intrusion Detection System Framework for Cloud Computing Networks. In: IEEE 39th International Conference on Parallel Processing Workshops, pp. 1–5. IEEE press (2010)
2. Dhage, S.N., Meshram, B.B., Rawat, R., Padawe, S., Paingokar, M., Mishra, A.: Intrusion Detection system in Cloud Computing Environment. In: ICWET 2011 Proceedings of the International Conference & Workshop on Emerging Trends in Technology, pp. 235–238. ACM, NY (2011)
3. Ranchal, R., Bhargava, B., Othmane, L.B., Lilien, L., Angin, P.: An Entity-centric Approach for Privacy and Identity Management in Cloud Computing. In: 29th IEEE symposium on Reliable Distributed Systems, pp. 177–183. IEEE press (2010)
4. Bugiel, S., Nürnberger, S., Sadeghi, A., Schneider, T.: Twin Clouds: An Architecture for Secure Cloud Computing. In: Workshop on Cryptography and Security in Clouds, ECRYPT II, the European Network of Excellence in Cryptology, and TClouds (2011)