Chapter 28
Comparing Single Tier and Three Tier Infrastructure Designs against DDoS Attacks

Akashdeep Bhardwaj
University of Petroleum & Energy Studies, Dehradun, India

Sam Goundar
CENTRUM, Graduate Business School, Lima, Peru

ABSTRACT

With the rise in cyber-attacks on cloud environments like Brute Force, Malware or Distributed Denial of Service attacks, information security officers and data center administrators have a monumental task on hand. Organizations design data center and service delivery with the aim of catering to maximize device provisioning & availability, improve application performance, ensure better server virtualization and end up securing data centers using security solutions at internet edge protection level. These security solutions prove to be largely inadequate in times of a DDoS cyber-attack. In this paper, traditional data center design is reviewed and compared to the proposed three tier data center. The resilience to withstand against DDoS attacks is measured for Real User Monitoring parameters, compared for the two infrastructure designs and the data is validated using T-Test.

INTRODUCTION

Modern day cybercrime attacks are specific, targeted and designed to compromise high-value customer data, including personal, financial and corporate intellectual property. Distributed denial of service attacks are not just aimed to bring down network infrastructure, hog bandwidths or compromise applications, there is a bigger danger lurking behind these attacks targeting data security. Modern day Data center designs have evolved in recent times, migrating from in house, private hosting centers with physical servers to hybrid clouds, spread across multiple locations with Software Designed Networks (or SDNs), virtualized hosts, Application Centric Infrastructure (or ACIs) running automation for IT recovery, de-

DOI: 10.4018/978-1-7998-5348-0.ch028

tection tasks, accelerating application deployments in dynamic manner with DevOps policy model for network, storage, servers and services. Designing secure data centers has now becoming mandatory as well as challenging.

The motivation to perform this research firstly aims at designing a secure data center architecture, secondly with security implementations being highly complex, one off customized implementations as per client requirements, network architects and cloud providers tend to lean towards accelerating application and service delivery, dynamic scalability, resource availability, reduced operating costs and increasing business agility. The cloud providers tend to keep security on low priority which results in security gaps that impacts security and performance. As per the research performed, real time protection, Internet peering or use of dedicated protection technology right at the Data Center edge routers checking the inbound traffic seems to be the best way for proactively mitigating DDoS attacks targeting business which is proposed in this research paper.

LITERATURE SURVEY

Lonea at al. (2013) deployed a virtual machine based intrusion detection with graphical interface to monitor cloud fusion alerts by using Eucalyptus cloud architecture for front end and MySQL database for backend. Attacks are captured by Barnyard tool while using SNORT for signature based DDoS rules. Stacheldraht tool is utilized for generating the resource depletion data packets. These packets consist of UDP, TCP SYN and ICMP floods. These attack packets are captured during the attack and stored in the central MySQL database. However, a limitation in this signature based approach is that unknown or zero day attacks could not be detected.

Bakshi et al. (2010) proposed an Intrusion Detection based on Signature detection for DDoS by using virtual machines running SNORT to analyze both the real time in-bound and out-bound traffic. The defense framework identifies the attacker's IP Address and auto scripts an Access Control List configuration for dropping the entire packets from that IP Address and blacklisting it immediately.

Gul et al. (2011) have cited that to handle a large packet flow, an intrusion detection model that analyzes and reports on the attack packets is utilized. These reports should be shared with the cloud actors involved. To improve the performance of the Intrusion Detection System multi-threading techniques are used. The final evaluation concluded that the use of multi thread deployment as compared to a single threaded deployment is more efficient.

Zarepoor at al. (2014) proposed the use of a statistical filtering system with two levels of filtering. The first level of filtering involves removing the header fields of incoming data packets, then comparing the time to live (TTL) value with a predetermined hop count value. If the values are not similar, the packet is termed to be spoofed and immediately dropped. The second level of filtering involves comparing the incoming packet header with a stored normal profile header.

Zakarya (2013) proposes an entropy based detection technique that identifies attack flow based on distribution ratio using the attack packet dropping algorithm. The entropy rate identifies the attack flow, dropping the packets if the DDoS is confirmed. Cloudsim simulation shows an accuracy of almost 90%.

Vissers et al. (2014) utilize Gaussian Model to preform defense against application layer attacks on cloud services using the parametric technique. The use of malicious XML content in use requests inside SOAP resulted in the DDoS attacks. Initially the detection involves HTTP header inspection to detect any HTTP floods and SOAP action inspection. Then XML content processing action is checked