Chapter 20
Algorithm for Secure Hybrid Cloud Design Against DDoS Attacks

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

Sam Goundar
https://orcid.org/0000-0001-6465-1097
Victoria University of Wellington, New Zealand

ABSTRACT

This article describes how cloud computing has become a significant IT infrastructure in business, government, education, research, and service industry domains. Security of cloud-based applications, especially for those applications with constant inbound and outbound user traffic is important. It becomes of the utmost importance to secure the data flowing between the cloud application and user systems against cyber criminals who launch Denial of Service (DoS) attacks. Existing research related to cloud security focuses on securing the flow of information on servers or between networks but there is a lack of research to mitigate Distributed Denial of Service attacks on cloud environments as presented by Buyya et al. and Fachkha, et al. In this article, the authors propose an algorithm and a Hybrid Cloud-based Secure Architecture to mitigate DDoS attacks. By proposing a three-tier cloud infrastructure with a two-tier defense system for separate Network and Application layers, the authors show that DDoS attacks can be detected and blocked before reaching the infrastructure hosting the Cloud applications.

1. INTRODUCTION

Hybrid Clouds offer the best-of-breed mitigation design options by combining the on premise, in house setup with specialized, third party DDoS mitigation. This combination provides an integrated mitigation solution. By utilizing a dedicated DDoS mitigation provider, the ability to detect and block multiple DDoS vectors or even have a Public Cloud provider dynamically increase the network pipe bandwidth

DOI: 10.4018/978-1-7998-2466-4.ch020

during a DDoS attack. Additionally, Hybrid clouds provide time and redundancy due to multiple tiers. Since the user and attacker's traffic is routed among multiple devices and tiers, the blocking and mitigation has option to initiate multiple checkpoints. This provides extra time after the attack is detected. With multiple layers, high availability and business continuity planning is achieved. This in turn helps save the infrastructure from the attack and prevents the effect on the availability of its online services.

Typical solutions during DDoS attack as presented by Buyya et al. (2017) and Phan et al. (2016) range from the entire traffic being diverted to a DDoS mitigation provider's cloud, where it is scanned, scrubbed with the attack traffic getting identified and removed before being re-routed back to the in-house data center of the enterprise as proposed by Fachkha et al. (2015). Cloud service providers like Rackspace Cloud Insights (Hybrid Cloud Blog, 2017) and Sify Cloud Blog (Hybrid Cloud Popularity, 2017) offers enterprises a comprehensive defense while delivering the most extensive range of security layers, high scalability with device and vendor independence for each tier and delivering the highest level of optimized performance in terms of network utilization and availability response. Based on the growing number of threats and impact of attacks, corporate enterprises having their own cloud services as well as cloud providers implement DDoS mitigation utilizing Hybrid Cloud Architecture as described by Ajagekar et al. (2017) and Girma et al. (2015). With the multi vector DDoS attacks, Layers 3, 4 and 7 are used to protect against volumetric, application and encrypted attack vectors, to detect, mitigate and have different mitigation tactics as proposed by Apiecionek et al. (2014), Banafar et al. (2014) and Hameed et al. (2016). This is achieved by use of multiple public cloud tiers, whose inherent features cover scalability to take on attack floods as presented by Jingle et al. (2014). The defense tiers act as first level of defense against network as proposed by Jain et al. (2014) and web application attacks presented by Jain et al. (2106). This allows hosting SaaS application, web portals and backend database to reside a controlled secure in-house private data center.

2. PRELIMINARIES

The authors recommend implementing a defense in depth approach, with a combination of interactive cyber protection technologies to provide a multiple layered defense, including implementing the following:

- Rate control threshold for devices with alerts and escalations
  - Inspection of multiple HTTP transactions
  - Detection over a short period of time
  - Triggers on excessive rate of client requests
- Web Application Firewall (WAF) behind network firewall
  - Inspection of single HTTP transactions
  - Attack detection in real-time
- Client reputation monitoring
  - Stop malicious actors at the source
  - Behavioral analysis on all cloud platform logs
  - Triggers on malicious intent to forecast potential attacks