Alok Verma et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 4, Issue 3, Sept 2017, pp. 226-228

Advanced Load Balancer and Reverse Proxy in Web Architecture

Alok Verma, Dr. Vivek Jaglan, Ankit Garg, Akshat Agarwal

Amity University, Gurgaon

***Abstract*—Load Balancer and Reverse Proxy have many similar features and are regressively used in IT industry to manage client load coming via internet to our backend or http servers. Also, these servers are exposed to internet vulnerability, so in that case the load balancer and reverse proxy servers come handy as they not only filter the incoming requests onto backend servers. But they also hide the server information getting exposed over internet. Which saves the servers from cyber-attacks and getting compromised.**

***Keywords* -Role and Importance of Load Balancer and Reverse Proxy**

I. INTRODUCTION

Load balancer's core role is to distribute the load across all the servers containing the same data or hosting the same content. Which not only helps to utilize the resource equally also prevents the over loading of requests onto any particular server. Which not only helps to make website more reliable but reduces the load across all server, also it helps in eliminating single point of failure, as if one node in a cluster is down then it auto detects the server and distribute the load of that server across other. Which reduces the single point of failure chances too [4].

A heap balancer likewise improves the client encounter by diminishing the quantity of mistake reactions a customer gets. It accomplishes this by distinguishing when a server goes down it occupies the solicitations far from them to alternate servers in the gathering. A heap balancer identifies the server wellbeing by observing the demand reaction to the general solicitations, additionally the heap balancer sends isolate wellbeing check solicitations to recognize the server wellbeing.

Another valuable capacity gave by stack balancers is session industriousness, which implies a heap balancer monitors every one of the solicitations landed onto which servers from specific customer. In spite of the fact that HTTP is stateless in principle, numerous applications must store state data to give center usefulness Ex-A shopping basket application where a server serves demands from just those customers whose solicitations it at first served amid confirmation and session creation. On the off chance that the heap balancer doesn't identify the session and disperses the demand regardless of session constancy crosswise over servers. Which will lead in disappointment of use.

II. UNDERSTANDING INTERNET PROXIES

- Reverse Proxies broker connections which are generally used in our load balancers are to handle requests coming from the internet, to our application servers [1,7].
- Forward Proxies are used in firewall which filter connections going out to the internet, from clients sitting behind the firewall. For example, if a user wants to access a shopping cart application from his work location, then his request will go to internet via work location's forward proxy. Which can either block or allow his requests.

Switch Proxies servers the approaching solicitations from the web and interface them to one server or bunch, which means numerous inbound associations from the web are pooled into at least one associations with the server(s). This is known as TCP Multiplexing, and is frequently utilized with Load Balancing systems to advance and quicken application conveyance.

Turn around Proxies measures stack in view of the approaching and active association proportion. The higher the proportion, the better the execution. Turn around Proxies are a piece of industry characterization Application Delivery Controller (ADC), or Application Delivery Network (ADN)..

III. REVERSE PROXIES

- Reverse proxies can operate wherever multiple web-servers must be accessible via a single public IP address.
- A invert intermediary can advance the backend server content by compacting the substance with a specific end goal to accelerate stacking time. It doesn't affect any information demand or reaction, yet it accelerates the execution.
- Reverse Proxies has capacity to perform TCP Multiplexing. It ends the approaching association, pools and builds up the new association toward the back utilizing less number of server associations which brings about a TCP Multiplexing Ratio. By and large, TCP Mux proportion is 10:1 – ten approaching associations with 1 back-end association.
- Reverse intermediary keeps the associations toward the back open notwithstanding when the approaching associations end so that these backend associations can be re-utilized when new approaching associations come in, which helps in diminishing an opportunity to build up server associations and brings about enhancing the execution [5].

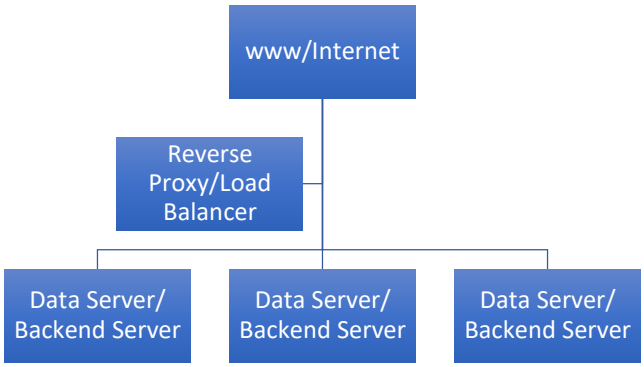

Figure 1

IV. Features of Reverse Proxy

- Application Delivery: Load Balancing (TCP Multiplexing)- It's responsible to sending the responses to the clients via Web Servers. Multiple clients can request the same content, so it distributes the load equally across all web server and delivers the response.
- Increased security – No backend server data is obvious outside inside system, so noxious customers can't get to data specifically to abuse any vulnerabilities. Turn around intermediary servers underpins highlights that assistance shield backend servers from circulated disavowal of-benefit (DDoS) assaults, case by boycotting IP address which doesn't enable that IP to send activity to backend framework any longer (boycotting), or constraining the quantity of associations acknowledged from every customer [2,6].
- SSL end – By decoding approaching solicitations and scrambling active solicitations turn around intermediary spares parcel of asset which can be utilized for fundamental reason and increment the execution [5,6].
- Caching – Before restoring the backend server's reaction to the customer, the turn around intermediary stores a duplicate of it locally. At the point when the customer makes a similar demand, the turn around intermediary can give the reaction itself from the store as opposed to sending the demand to the backend server. This the two abatements reaction time to the customer and decreases the heap on the backend server [6].
- Increased adaptability and adaptability – As customers can't see backend framework, framework proprietors are allowed to change the design of backend foundation. This is valuable in a heap adjusted condition, where number of servers can be changed to meet activity necessity [6].

SSL Offload/Acceleration (SSL Multiplexing) – Reverse Proxy reserves the information and

- Caching
- Compression
- Content Switching/Redirection
- Application Firewall
- Server Obfuscation
- Authentication
- Single Sign On
- Reverse intermediaries shrouds the presence and qualities of backend servers and it and it spares it from any assault from web.
- A invert intermediary can add fundamental HTTP validation to a web server.

In request to influence site to secure SSL encryption can be performed at Load balancer or Reverse Proxy level rather than webserver level. Rather, if a client tries to perform SSL at webserver level then they may need to perform over all the webservers dealing with customer demands. Which can be colossal in number. Likewise, an invert intermediary server or load balancer can be furnished with SSL quickening programming additionally [3,7]. A switch intermediary conveys the heap from approaching solicitations to a few servers, with every server serving its own particular application territory. The turn around intermediary can likewise revamp the URL in every approaching solicitation from the web or other asset with a specific end goal to coordinate the inward area of the asked for asset. A invert intermediary or load balancer can diminish stack on its servers by reserving static and dynamic substance which is regularly named as web speeding up. The Reverse Proxy reserves and serves various site demands which brings about diminishing the heap over genuine backend server.

Reverse Proxy Limitations and Solutions

- If the reverse proxy is compromised and a failover is not in place, the site will remain unavailable for all clients.

V. Conclusion

Since in case of failover the complete reverse proxy server, the reverse proxy servers are coming up features of auto reset to default settings. Also, netting between the public IP and the reverse proxy server can be changed to new reverse proxy server. Which in turn will point to existing backend http servers. If an outside attacker compromises the reverse proxy server, the attacker will be able to gain access to http servers configured at the backend.

We can restructure the architectures of our backend system, where we can have multiple reverse proxy server or load balancers in tree structure, which in fact work as multi-layer gateway for an attacker and it saves the system from getting compromised.

REFERENCES

[1]. https://networkengineer.me/2014/06/08/reverse-proxy-reverse-proxy-vs-forward-proxy/
[2]. https://www.nginx.com/blog/mitigating-ddos-attacks-with-nginx-and-nginx-plus/
[3]. https://www.nginx.com/resources/glossary/reverse-proxy-server/

[4]. https://en.wikipedia.org/wiki/Load_balancing_(computing)
[5]. https://en.wikipedia.org/wiki/TLS_termination_proxy
[6]. https://www.nginx.com/resources/glossary/reverse-proxy-vs-load-balancer/
[7]. https://en.wikipedia.org/wiki/Reverse_proxy

