1st International Conference on Applied Soft Computing Techniques
22 & 23.04.2017
In association with
International Journal of Scientific Research in Science and Technology

Secure Socket Layer Based Load Balancing Methodology In Distributed Servers

[1] G. Srilakshmi,[2] Dr. K. Kungumaraj
[1]Department of Computer Science, Mother Teresa Women's University, Kodaikanal, TamilNadu, India
gsrilakshmi.gsl@gmail.com[1]
[2]Department of Computer Applications, Arulmigu Palaniandavar Arts and Science College for Women, Palani,TamilNadu,India
kungumarajkalimuthu@gmail.com [2]

ABSTRACT

A SSL load balancer goes about as the server-side SSL endpoint for associations with customers, implying that it plays out the decoding of solicitations and encryption of reactions that the web or application server would some way or another need to do. The procedure differs fairly relying upon the security of the system between the heap balancer and server. On the off chance that the heap balancer and server are on the same secured organize (for the most part this implies being behind a firewall), the SSL load balancer is typically arranged to unscramble the demand, separate the data required for load adjusting, and forward the demand to the server free (decoded). It encodes the server's reaction before returning it to the customer. On the off chance that the system between the load balancer and server is not secure, the SSL load balancer is generally arranged to decode the demand, remove the data required for load adjusting, and re-encode the demand before sending it to the server. The procedure is turned around for the reaction from server to customer. Offloading the decoding and encryption handle, which is computationally serious, liberates web and application servers to play out the work they are intended for, which speeds content conveyance and enhances the general client encounter. In the event that the system between load balancer and servers is secure, you just need to introduce and deal with the SSL declarations on the load balancer rather than each web and application server. This fundamentally diminishes managerial overhead if the gathering of servers is expansive.

Keywords: Load balancing, SSL, SSL Methodology, Load balancing Techniques

I. INTRODUCTION

In a cluster based server pool or network server, all solicitations from customers to an application server are initially passed to a wholesaler from a Web switch and after that the merchant advances each demand to one of the application servers as indicated by its circulation approach. The circulation in the application server ought to be done another way contrasted with the front-level Web server in which a store mindful conveyance like Locality-Aware Request Distribution indicates great execution. Particularly because of the high overhead of the SSL convention, the wholesaler in an application server ought to embrace an arrangement that limits the SSL overhead. Since the session reuse conspire, which is broadly utilized as a part of single Web servers, is exceptionally viable to diminish the SSL overhead, the specialist plan to misuse the session reuse plot for the group based application servers.

The distributor of SSL-Session calculation keeps up the customer data to forward resulting demands from a similar customer to a similar application server. The upside of the SSL-Session is that it stays away from the pointless verification and arrangement stage when a customer tries to reconnect to the server. The weakness of this model is that it might bring about load awkwardness among the servers. On the off chance that a server has customers whose solicitations are visit and require much element calculation, the solicitations can't be disseminated to other gently stacked servers, bringing about load skewness among the servers. The fundamental disadvantage in the current technique is time idleness. The server load couldn't be adjusted

because of capricious heap of the intermediary servers. The current framework neglects to query way length and the quantity of overwhelming hubs experienced in every way. The metric of way length mirrors the execution of the question sending plan, and the metric of number of overwhelming hubs indicates how the blockage control convention maintains a strategic distance from substantial hubs in direct activity stream.

The system developed using Round Robin and SSL-Session model are not effective. Those models are not able to give the output in time and the throughput also lesser than that the expected output. Round Robin and SSL-Session models had the latency problem and minimal throughput. For this reason, the researcher introduced the SSL-LB load balancing model. The following are the drawbacks in the existing system:

1. In the existing system, users need to spend more time for retrieving their data.
2. Time consuming
3. Latency Problem
4. Minimum Throughput

II. SSL-LB METHODOLOGY

The SSL-LB model is aimed at mitigating the limitation of SSL-Session by using a new load balancing mechanism to achieve load balancing. The SSL-LB load balancing module get the load information from each application server and navigate the client request to the lightly loaded application server.

For effective load balancing, this examination presents Secure Socket Layer plot, which is utilized to associate the customer with the intermediary servers. Proficient diverting can be made by the server when a client asks for at the server top time. SSL-LB strategy will decrease the idleness time and increment the throughput than the current framework (Round Robin display and SSL-Session). The SSL-LB will lessen the server pay stack and enhances the throughput while the server is being occupied.

SSL-LB, which operates between the HTTP and Transmission Control Protocol (TCP) network layers, is the most popular tool that provides a secure channel between a client and a Web server. SSL-LB is composed of two components: a handshaking procedure and a bulk data encryption procedure. A client initiates a connection with a server by sending a Client Hello message that includes the session ID, a random number, cipher suites, and other required information. After receiving the Client Hello, the server sends a Server Hello including its certificate and other information as a reply. With the certification of the server, the client finishes the authentication of the server. Depending on the server side configuration, the next procedure for the client authentication is optional. If it is requested, the client needs to send the certificate to the server for verification. After the authenticating procedures, the client generates session keys for the encryption and decryption of data. The session is identified by the session ID that is shared between the clients and server.

The main aim of this research is to reduce the pay load of the Web server. The server load balancing methods such as Random walk algorithm, Round Robin [RR] model, SSL-Session model and SSL-LB are reducing the server pay load. Random walk algorithm does not consider the load in the system and selects a random node and execute the processes with reduced throughput. The Round Robin scheduling does not acknowledge priorities, and does not allow out-of-order processing. SSL-Session may expire in a short duration of time.

III. SYSTEM MODEL

There are different servers introduced in geologically found spots and SSL-LB disseminates the clients demand to the suitable server and diminishes the compensation heap of the server. The SSL-LB has been displayed thusly as it were.

The incorporated Web and application server acts as takes after: The solicitations from client procedures are circulated by the distributor to the servers. When a server gets a demand, it opens a SSL association with the client. On the off chance that the server has the customer's past session data, it avoids the RSA lopsided key operation. As per the demand sort (static or element), the demand is prepared in an unexpected way. In the event that the demand is for static substance, it is adjusted by the Web server module. Else, it is sent to the application server module. The application server conjures the correspondence module to send the demand to another hub.

The below Figure 1 represents the SSL-LB system model. End-user requests are sent to a SSL-LB load-balancing system that determines which server is most capable of processing the request. It then forwards the request to that server. Server load balancing can also distribute workloads to firewalls and redirect requests to proxy servers and caching servers.

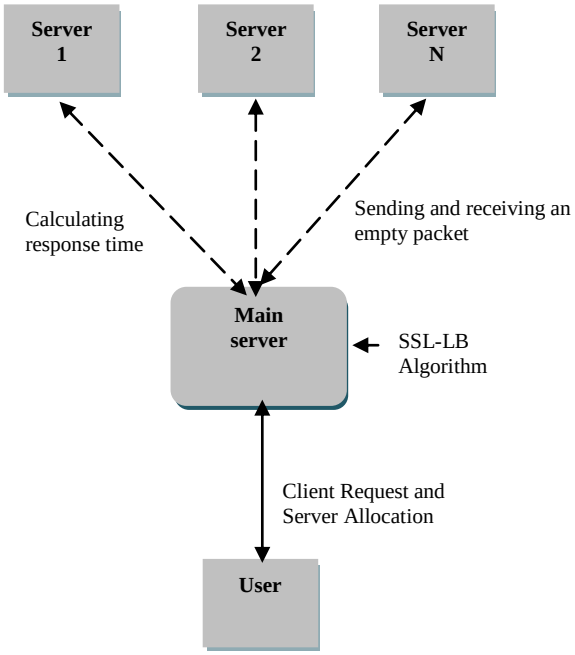

Figure 1: SSL-LB System Model

The Figure 2 represents outline of the load balancing system which is navigating the user requests to the sub-server when the main server is busy. Client's request sent to the load balancing system and load balancer calculate the response time for sub-servers. Based on the response time, the particular lightly loaded sub-server will be allocated to the client. This system has been modeled using various steps such as entry module, server representation, sharing resources and connecting clients with the sub-servers.

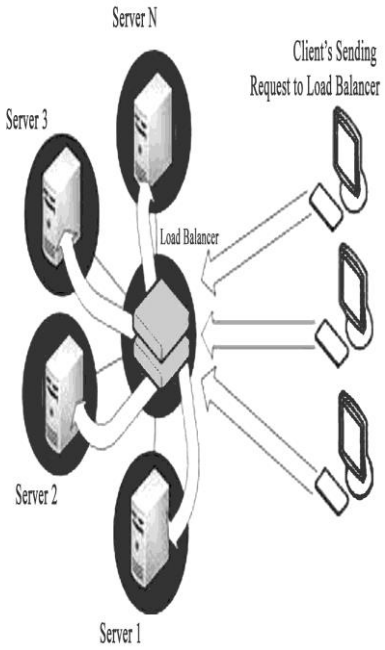

Figure 2: Outline of Load Balancing System

IV. SSL-LB IMPLEMENTATION

The source control program is operating similar to visual source safe. It performs sensibly easy by getting to the customer to set out refreshed data all the while. Generally it is completed utilizing Visual Studio.net or Front Page for assessment. At the point when every one of the procedures keep running on the group based server, the key capacity is load adjusting. Assume any one server in the cluster may harm, then the NLB cluster will re-balance the currently access request to continue the further operation. The principle favorable position of this strategy is that there is no connection between the servers in the cluster; consequently the impacts in one server won't influence the other server in the group.

Input text document is given by administrator and the scrambled arrangement is put away in all servers. The load balancing of the system technique will assembled a ranch of server. This server cultivate contains undesirable group getting to a few server benefit on a solitary IP address. Output module is a decrypted file from the server which is out of gear state. Yield module produces reaction time graph. The Network Load Balancer [NLB] handle the server related program and each approaching sign is acknowledged by every one of the hubs, however just the server with light load, will reaction rapidly. NLB apportions sub-server with less response time to the client who makes the demand.

Another advantage of the network load balancing scheme can gives idea of how much percentage of load balancing can be performed and find how the load can be shared within the nodes in the cluster. With the help of this load percentage calculation, it is very easy to select and transmit the data through the lightly loaded server. The user constantly distributed to the all nodes of the Web server, so that it is possible to find the percentage of load among the servers. In this case, the load of the server will change periodically during the request sending and receiving to the server. But in SSL-Session backend forwarding scheme, the load balance will be constant factor, hence there is no possibility of variance.

For applications, such as servers, this has numerous clients and relatively short-lived client requests. The ability of Network Load Balancer is to distribute workload efficiently and provides fast response to cluster changes. The network load balancing cluster will send the request to the all the node in the network, and looking for the response. Suppose the response did not receive from any other nodes, it shows the node will not function properly. From this idea, it is automatically re-arrange the server in the node. Every server in the cluster based application provides high level of security. Except database, it can be able to operate along and it does not need any other server for support. The server can be configured separately and execute the server operation without any help from other server. But in case of static Web server, it is not possible to run HTML file separately and there must be a problem raised when support file missing.

A. START SSL-LB

SSL-LB session is a logical connection between a client or server application over a Transmission Control Protocol (TCP) socket by using the SSL protocol. The SSL application creates a TCP socket, starts the TCP connection, and then starts the SSL-LB session over the TCP connection. The SSL-LB session is mapped to the TCP socket, therefore if the socket fails, the SSL-LB session will fail. When the SSL application sends data, the data is encrypted by the SSL code and sent across the TCP socket to the remote node. The SSL code in the remote node reads the data from the TCP socket, decrypts the data, and passes the data to the SSL application.

B. SSL-LB HANDSHAKE

SSL-LB session always begins with an exchange of messages called an SSL-LB handshake. The SSL-LB handshake allows the server to authenticate itself to the client by using public-key techniques. It should allow the client and server to cooperate in creating symmetric keys that are used for encryption, decryption, and tamper detection during the SSL-LB session that follows. The SSL-LB handshake can also allow the client to authenticate itself to the server.

C. END SSL-LB

To end SSL-LB session gracefully, it is ended before the Transmission Control Protocol (TCP) socket is ended. The client and server applications issue the SSL-shutdown function, which causes the SSL-LB session shutdown alert to flow across the TCP socket to the remote node. After the client and server applications have issued the SSL-shutdown function, the SSL-LB session is ended and the applications can then close the TCP socket

D. SSL-LB CONNECTION

1) Connection: It is client and server logic link; it associated with provision of suitable types of server. In SSL-LB terms, it must be a peer-to-peer connection.

2) Session: An association between client and server that define a set of parameter such as algorithm used.

The SSL-LB Session created by Handshake protocol that allows a parameter to be shared among the connection between client and server, and session is used to avoid negotiation of new parameters of each connection. A single session is shared among multiple SSL connection between client and server. SSL-LB session and connection involves several parameters that are used for SSL-LB enable communication between client and server. During the negotiations of the handshake protocol, the encryption methods are established and a series of parameters the session state are subsequently used within the session. Mostly SSL protects the HTTP communication channel over the internet and therefore the SSL protocol is seen quite often as associated only with www pages. The SSL protocol can be used to protect the transmission for any TCP/IP service.

V. CONCLUSION

Server load balancing is a powerful technique for improving application availability and performance in service provider, Web content provider and enterprise networks but implementation can also increase network cost and complexity. There are various servers introduced in geologically found spots and SSL-LB conveys the customer's demand to the suitable server and diminishes the compensation heap of the server. Extraordinary Networks gives the key advantages of server load balancing while dispensing with the potential cost, multifaceted nature, and execution issues.

VI. REFERENCE

[1] P Rafiq, J Kann: Network Load Balancing and Its Performance Measures, published on May 19,2015. International Journal of Computer Science Trends and Technology (IJCST) – Volume 3 Issue 1, Jan-Feb 2015. ISSN: 2347-8578.

[2] Dipesh Gupta, Hardeep Singh: Review on TLS or SSL session sharing based web cluster load balancing. In proceedings of International Journal of Research in Engineering and Technology.Volume: 03 Issue: 11, Nov-2014. ISSN: 2321-7308.

[3] Web server load balancing using SSL back-end forwarding method V. M. Suresh; D. Karthikeswaran; V. M. Sudha; D. Murali Chandraseker IEEE – International Conferences on Advances in Engineering, Science and Management (ICAESM-2012).

[4] Jin-Ha Kim, 2007. An SSL Back-End Forwarding Scheme in Cluster Based Web Servers. IEEE transactions on parallel and distributed systems, 18(7):946-957. ISSN: 1045-9219.

[5] JH Kim, GS Choi, CR Das: A Load Balancing Scheme for Cluster-based Secure Network Servers, proceedings in IEEE International Conference On Cluster Computing, on September 2005, pp. 1-10.

[6] Shilpi pandey,Shivika prasanna : Load Balancing Techniques: A Comprehensive study published on April 2015,International journal of Advance research in Computer science and management studies, Volume 3,Issue 4,ISSN:2321-7782