International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015
ISSN 2091-2730

An Enhanced B+ Packet Search for Cloud Network Security

Kirubakaran.R[1], Jayakumar.D[2], Sivachandiran.S[3]

[1]PG Final Year Student, Department of MCA, IFET College of Engineering

Villupuram, Tamilnadu, India

E-mail: kirubaifet@gmail.com

Mobile Number: 8098746799

[2]Assistant Professor, Department of CSE, IFET College of Engineering

Villupuram, Tamilnadu, India

E-mail: jayakumar1988@hotmail.com

Mobile Number: 9600607743

[3]Assistant Professor, Department of MCA, IFET College of Engineering

Villupuram, Tamilnadu, India

E-mail: sivachandiran.s@gmail.com

Mobile Number: 9940738523

Abstract - Many researches show that virtualization and cloud computing are technologies that will be essential in the future. They are already widely used because of the many advantages they introduce. They permit to reduce hardware cost, reduce the energy consumption, and ease the management of an ever-growing number of computers and servers. However, this abrupt switch from physical infrastructures to virtualized ones introduces a new networking aspect, the virtual traffic, and poses the question of how to secure this new type of traffic. In fact, virtual traffic between two virtual machines may never leave the physical host hardware; making traditional physical firewalls useless to monitor and secure this traffic. The best solution to this problem is the use of virtual firewalls. The aim of this project is to evaluate the performances of a virtual firewall in a cloud environment. This thesis reviews the literature in the field of cloud computing and virtual firewall and concludes that three key requirements must be met in order to realize an effective evaluation: the choice of a cloud infrastructure, the choice of meaningful evaluation metrics and the use of proper evaluation methodologies.

Keywords - *Cloud computing, energy consumption, Time consumption, Firewall, Cloud Environment, Packet Search, effective evaluation.*

INTRODUCTION

Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications.

FIREWALL

A firewall is a network security system, either hardware or software based, that controls incoming and outgoing network traffic based on a set of rules. Acting as a barrier between a trusted network and other untrusted networks such as the Internet or less trusted networks such as a retail merchant's network outside of a cardholder data environment -- a firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network defined in the firewall policy is; all other traffic is denied. When connected to the internet, even a standalone PC or a network of interconnected computers make easy targets for malicious software & unscrupulous hackers. A firewall can offer the security that makes you less vulnerable and also protect your data from being compromised or your computers being taken hostage.

TYPES OF FIREWALL

1) Software firewalls

New generation Operating systems come with built in firewalls or you can buy a firewall software for the computer that accesses the internet or acts as the gateway to your home network.

2) Hardware firewalls

Hardware firewalls are usually routers with a built in Ethernet card and hub. Your computer or computers on your network connect to this router & access the web.

HOW DO THEY WORK?

Firewalls are setup at every connection to the Internet therefore subjecting all data flow to careful monitoring. Firewalls can also be tuned to follow "rules". These Rules are simply security rules that can be set up by yourself or by the network administrators to allow traffic to their web servers, FTP servers, Telnet servers, thereby giving the computer owners/administrators immense control over the traffic that flows in & out of their systems or networks.

Rules will decide who can connect to the internet, what kind of connections can be made, which or what kind of files can be transmitted in out. Basically all traffic in & out can be watched and controlled thus giving the firewall installer a high level of security & protection.

LITERATURE REVIEW

Shadowed rule (i.e., a rule that may never be matched by any packet as a result of the packet should have matched with alternative rules above) will cause security and speed problem;swapping position between rules changes the firewall policy and thence causes a security problem; ‘redundant rules’ will cause speed problem; firewall directors got to find ‘bigger rules’ solely once ‘smaller rules’, and this ends up in a ‘difficult to use’ problem; and sequential rule looking out will cause a speed drawback.

DESIGN OF MODEL

- It includes the cloud server environment where the client machines can be added one after the other through valid login. Any client working through his/her can request stored information for processing from the cloud. Once the details are requested from the part of the client, possibly the data is forwarded from the server to the client through cloud storage unit.
- Processing of server to client communication is formulated in our project Server chooses necessary data to be transferred and specifies the desired client machine where the data is to be delivered. The information transfer initiates from the cloud server, reaches through the intermediate cloud medium and finally gets on delivered to the client unit.

ARCHITECTURE DIAGRAM

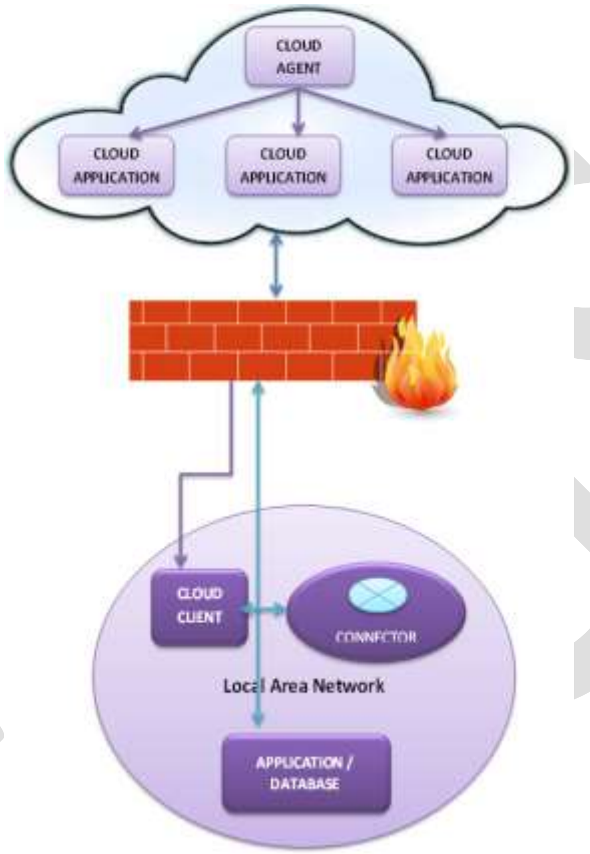

Fig 1.Firewall Architecture

EXISTING SYSTEM

In existing system they use binary search to find the IP Address .This may take long time but they achieve it.

DISADVANTAGES OF EXISTING SYSTEM

- Severity of Exposing the Security Issues
- Error prone to Speed Drop
- Due to Swapping of Position, the policy of firewall is affected.

BINARY SEARCH

Binary search or half-interval search algorithm finds the position of a specified input value (the search "key") within an array sorted by key value. For binary search, the array should be arranged in ascending or descending order. In each step, the algorithm compares the search key value with the key value of the middle element of the array. If the keys match, then a matching element has been found and its index, or position, is returned. Otherwise, if the search key is less than the middle element's key, then the algorithm repeats its action on the sub-array to the left of the middle element or, if the search key is greater, on the sub-array to the right. If the remaining array to be searched is empty, then the key cannot be found in the array and a special "not found" indication is returned.

PROPOSED SYSTEM

Our proposal is using B+ instead of using Binary search. This can make search speed higher. The B+ search is the best search a particular node in a tree.

B+ Search

B+ tree is an n-array tree with a variable but often large number of children per node. A B+ tree consists of a root, internal nodes and leaves. The root may be either a leaf or a node with two or more children. The root of a B+ Tree represents the whole range of values in the tree, where every internal node is a subinterval.

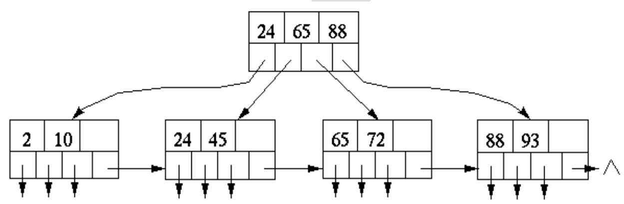

Fig 2. B+ Tree

ADVANTAGES OF PROPOSED SYSTEM

- We identify five limitations of traditional Listed-Rule firewalls on large networks.
- We propose and design a Tree-Rule firewall model that has none of the five limitations.
- We examine Tree-Rule firewalls on LANs and demonstrate better performance than IPTABLES.
- We show efficient performance and benefits of Tree-Rule firewalls under a cloud environment.

MODEL AND MECHANISMS

RULE ANALYSIS

We only compare the throughput of IPTABLES and Tree-Rule firewall because thousands of IPTABLES rules can be created using shell scripts, and the rules for a Tree-Rule firewall undera cloud environment can easily be produced by modifying our source code written for the GUI of Tree-Rule firewall creation . Because the proposed Tree-Rule firewall has three attributes (i.e., Source IP, Dest IP and Dest Port), its rules can be easily produced using a three layer programming loop.

BFS SEARCH

- In graph theory, breadth-first search (BFS) is a strategy for searching in a graph when search is limited to essentially two operations: (a) visit and inspect a node of a graph; (b) gain access to visit the nodes that neighbour the currently visited node. The BFS begins at a root node and inspects all the neighbouring nodes. Then for each of those neighbour nodes in turn, it inspects their neighbour nodes which were unvisited, and so on. Compare BFS with the equivalent, but more memory-efficient Iterative deepening depth-first search and contrast with depth-first search.
- The algorithm uses a queue data structure to store intermediate results as it traverses the graph, as follows:

- Enqueue the root node
- Dequeue a node and examine it
- If the element sought is found in this node, quit the search and return a result.
- Otherwise enqueue any successors (the direct child nodes) that have not yet been discovered.
- If the queue is empty, every node on the graph has been examined – quit the search and return "not found".
- If the queue is not empty, repeat from Step2.

No.	Source_IP	Dest_IP	Dest_Port	Action
1	200.1.2.99	200.1.1.3	22	Accept
2	200.1.2.99	200.1.1.4	22	Accept
3	200.1.2.*	200.1.1.2	22	Accept
4	200.1.2.*	200.1.1.5	22	Accept
5	200.1.2.*	200.1.1.3	110	Accept
6	200.1.2.*	200.1.1.3	143	Accept
7	200.1.2.*	200.1.1.5	3306	Accept
8	*	200.1.1.1	22	Accept
9	*	200.1.1.1	80	Accept
10	*	200.1.1.2	80	Accept
11	*	200.1.1.2	443	Accept
12	*	200.1.1.3	25	Accept
13	*	200.1.1.4	53	Accept
14	200.1.2.*	200.1.1.*	*	Deny
15	200.1.2.*	*	*	Accept
16	200.1.1.3	*	25	Accept
17	200.1.1.4	*	53	Accept
18	*	*	*	Deny

Fig 3.BFS Search

IMPLEMENTATION

DATA FLOW DIAGRAM

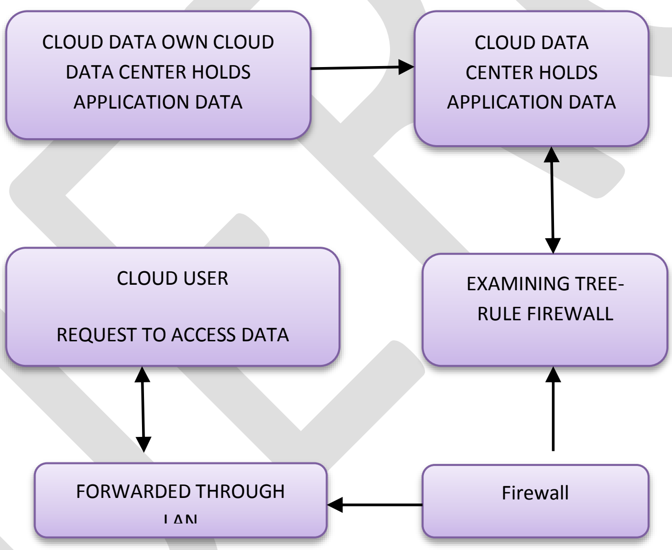

Fig 4. Firewall working system

Framework exhibits the safety issues that are presently handling this issue by cloud network. And therefore the security is major downside that is overcome by our model. Then he will transfer file from client to client and server to server.

In this project, one amongst the module names is cloud environment in this client will able to share their post with the assistance of the tree rule firewall model and to authorize the assorted labelled user to present permission. The permission involves 2 varieties they're permit and Deny. These offer the authorization to the client to share or read the files that the server shared with the indexed clients.

It provides fine strength of user friendly platform to create terribly easier to user. Csharp Dot application as front and Microsoft database information as a backend. Once the client registers with basic data, it saves the knowledge to information database. Each client behaviour and performance management of user is represent the activity of the live client in order that knowledge relating to client is store in information and pattern ought to be keep with them on each activity log of the client. The new client will send the request to the prevailing user; existing client will read the request for approval. User will transfer the files between client and server.

FUTURE ENHANCEMENT

For future work, we will study better combinations of partition and placement modules, understand the implementation constraints on network state information accuracy, and design online algorithms to handle network and rule dynamics.

CONCLUSION

Privacy preserving outsourcing of firewall services benefits ISPs and customers significantly; however, this is a very difficult technical problem. This paper makes the first step towards this new direction which makes to search packet in easy and fastest way.

REFERENCES:

[1]T.Ritter, “Network-based firewall: Extending the firewall into the cloud,”http://www.business.att.com/content/whitepaper/NemertesDN0496Network-Based FirewallServicesMay2009.pdf, 2009.

[2] “AT&T-Network-Based Firewall,” http://www.business.att.com/enterprise/Service/business-continuity-enterprise/ebfirewallsecurity/networkbased-firewall-enterprise/

[3] R. Richardson, “CSI/FBI computer crime and security survey,” 2008.

[4] M. Whitworth, “Outsourced security the benefits and risks,” Network Security, pp. 16–19, 2005.

[5]“Strategies for outsourcing security measures,”http://www.cisco.com/en/US/netsol/ns546/netvalueproposition09186a0080145ad7.html, 2002.

[6] J. Grady, “The little guy fights back: Outsourcing firewall management makes economic sense for smaller companies - service providers,” Telecommunications.(http://findarticles.com/p/articles/mi m0TLC/is136/ai83150961/),2002.

[7] “Survey: 88% of ICT Employees Would Steal,”http://www.scoop.co.nz/stories/BU0811/S00203.htm, 2008.

[8] R. B. McAfee and P. J. Champagne, Effectively managing troublesome employees. Quorum Books, 1994.

[9] M. G. Gouda and A. X. Liu, “Structured firewall design,” Computer Networks Journal (Elsevier), vol. 51, no. 4, pp. 1106–1120, March 2007.

[10] B. Bloom, “Space/time trade-offs in hash coding with allowable errors, “Communications of ACM, vol. 13, no. 7, pp. 422–426, 1970.[Online].

[11] J. Cheng, H. Yang, S. H. Wong, and S. Lu, “Design and implementation of cross-domain cooperative firewall,” in Proc. IEEE Int. Conf. on Network Protocols (ICNP), 2007.

[12] A. X. Liu and F. Chen, “Collaborative enforcement of firewall policies in virtual private networks,” in Proc. PODC, 2008.

[13] D. A. Maltz, J. Zhan, G. Xie, H. Zhang, G. Hj´ almt´ ysson, A. Greenberg,and J. Rexford, “Structure preserving anonymization of router configuration data,” in Proc. IMC, 2004.

[14] M. Harvan and J. Sch¨ onw¨ alder, “Prefix- and lexicographical-orderpreservingip address anonymization,” in 10th IEEE/IFIP Network Operations and Management Symposium (NOMS), 2006.

[15] R. Ramaswamy and T. Wolf, “High-speed prefix-preserving ip address anonymization for passive measurement systems, ”IEEE/ACM Transaction in Networking, vol. 15, pp. 26–39, 2007.

[16] R. Pang, M. Allman, V. Paxson, and J. Lee, “The devil and packet traceanonymization,” inProc. ACM SIGCOMM, 2006