ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

Smart Shop Search Android Mobile Application

[1]P.Gayathri, [2] A. Rama

[1,2]Asst.Professor, Dept of IT, Bharath Institute of Engg & Tech,Chennai – 73, India

ABSTRACT: The advent of rising computing technologies like service-oriented design and cloud computing has enabled US to perform business services additional with efficiency and effectively. However, we tend to still suffer from unintended security leakages by unauthorized actions in business services. Firewalls ar the foremost wide deployed security mechanism to make sure the protection of personal networks in most businesses and establishments. The effectiveness of security protection provided by a firewall in the main depends on the standard of policy organized within the firewall. sadly, coming up with and managing firewall policies ar typically error prone because of the complicated nature of firewall configurations likewise because the lack of systematic analysis mechanisms and tools.

we tend to represent associate degree innovative policy anomaly management framework for firewalls, adopting a rule-based segmentation technique to spot policy anomalies and derive effective anomaly resolutions. especially, we tend to articulate a grid-based illustration technique, providing associate degree intuitive psychological feature sense regarding policy anomaly. we tend to additionally discuss a proof-of-concept implementation of a visualization-based firewall policy analysis tool known as Firewall Anomaly Management surroundings (FAME). additionally, we tend to demonstrate however with efficiency our approach will discover and resolve anomalies in firewall policies through rigorous experiments.

I.INTRODUCTION

A one of essential elements in network and information system security, firewalls have been widely deployed in defending suspicious traffic and unauthorized access to Internet-based enterprises. Sitting on the border between a private network and the public Internet, a firewall examines all incoming and outgoing packets based on security rules. To implement a security policy in a firewall, system administrators define a set of filtering rules that are derived from the organizational network security requirements. Firewall policy management is a challenging task due to the complexity and interdependency of policy rules. This is further exacerbated by the continuous evolution of network and system environments. For instance, Al-Shaer and Hamed reported that their firewall policies contain anomalies even though several administrators including nine experts maintained those policies. In addition, Wool recently inspected firewall policies collected from different organizations and indicated that all examined firewall policies have security flaws.

II.LITERATURE SURVEY

Network Security is needed to prevent hacking of data and to provide authenticated data transfer[1]. Network Security can be achieved by Firewall. Firewall is a hardware or software device designed to permit or deny network transmissions based upon a set of rules and regulation. It is frequently used to protect networks from unauthorized access. A firewall is typically placed at the edge of a system and acts as a filter for unauthorized traffic[2]. But conventional firewalls rely on the notions of restricted topology and controlled entry points to function. Restricting the network topology, results in difficulty in filtering of certain protocols, End-to-End encryption problems etc. So distributed firewalls are used which allow enforcement of security policies on a network without restricting its topology on an inside or outside point of view. Distributed firewalls secure the network by protecting critical network endpoints, exactly where hackers want to penetrate. It filters

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

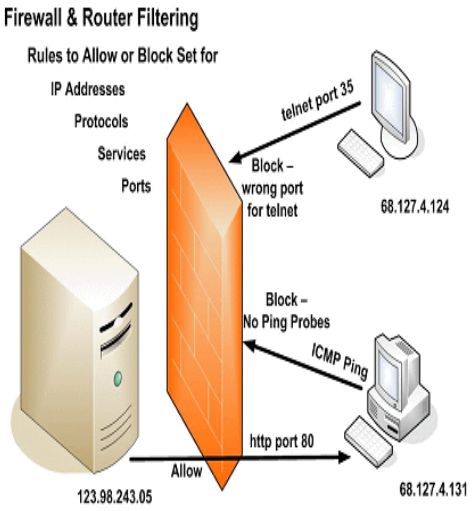
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

traffic from both the Internet and the internal network. They provide unlimited scalability and also they overcome the single point of failure problem presented by the perimeter firewall.

In today's world, most businesses, regardless of size, believe that access to the Internet is imperative if they are going to compete effectively. Even though the benefits of connecting to the Internet are considerable, so are the risks. Lots of data are getting transferred through it; one can connect any computer in the world to any other computer located apart from each other[3][4]. A number of confidential transactions occur every second and today computers are used mostly for transmission rather than processing of data. We need some approach to secure transmission of the data, by the concept of Network Security, which involves the corrective action taken to Ease of Use protect from
the viruses, hacking and unauthorized access of the data .It is a Network Security needed to prevent hacking of data and to provide authenticated data transfer. This Network Security can be achieved by Firewalls. A Firewall is a collection of components, which are situated between two networks that filters traffic between them by means of some security policies[5]. A Firewall can be an effective means of protecting a local system or network systems from network based security threats while at the same time affording access to the outside world through wide area networks and the Internet. Traditional firewalls are devices often placed on the edge of the network that act as a bouncer allowing only certain types of traffic in and out of the network. Often called perimeter firewalls. They divide the network into two parts-trusted on one side and untrusted. For this reason they depend heavily on the topology of the network. In general, firewalls can be categorized under one of two general types:

• Desktop or personal firewalls
• Network firewalls
Within the network firewall type, there are primary classifications of devices, including the following:
• Packet-filtering firewalls (stateful and nonstateful)
• Circuit-level gateways
• Application-level gateways



III.FIREWALL DEPLOYMENY

Communication between two hosts using a network may be encrypted to maintain privacy.
Honeypots, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the honeypot. A honeypot can also direct an attacker ' s attention away from legitimate servers. A honeypot encourages

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honeypot, a honeynet is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker ' s methods can be studied and that information can be used to increase network security. A honeynet typically contains one or more honeypots.

IV.. SYSTEM ANALYSIS

4.1EXISTING SYSTEM:

Firewall policy management is a challenging task due to the complexity and interdependency of policy rules. This is further exacerbated by the continuous evolution of network and system environments.

The process of configuring a firewall is tedious and error prone. Therefore, effective mechanisms and tools for policy management are crucial to the success of firewalls[7].

Existing policy analysis tools, such as Firewall Policy Advisor and FIREMAN, with the goal of detecting policy anomalies have been introduced. Firewall Policy Advisor only has the capability of detecting pair wise anomalies in firewall rules. FIREMAN can detect anomalies among multiple rules by analyzing the relationships between one rule and the collections of packet spaces derived from all preceding rules.

However, FIREMAN also has limitations in detecting anomalies. For each firewall rule, FIREMAN only examines all preceding rules but ignores all subsequent rules when performing anomaly analysis. In addition, each analysis result from FIREMAN can only show that there is a misconfiguration between one rule and its preceding rules, but cannot accurately indicate all rules involved in an anomaly.

DISADVANTAGES OF EXISTING SYSTEM:

Fireman can detect anomalies among multiple rules by analyzing the relationships between one rule and the collections of packet spaces derived from all preceding rules. For each firewall rule, FIREMAN only examines all preceding rules but ignores all subsequent rules when performing anomaly analysis[6].

4.2 PROPOSED SYSTEM:

We represent a novel anomaly management framework for firewalls based on a rule-based segmentation technique to facilitate not only more accurate anomaly detection but also effective anomaly resolution.

Based on this technique, a network packet space defined by a firewall policy can be divided into a set of disjoint packet space segments. Each segment associated with a unique set of firewall rules accurately indicates an overlap relation (either conflicting or redundant) among those rules.

We also introduce a flexible conflict resolution method to enable a fine-grained conflict resolution with the help of several effective resolution strategies with respect to the risk assessment of protected networks and the intention of policy definition[8].

ADVANTAGES OF PROPOSED SYSTEM:

In our framework conflict detection and resolution, conflicting segments are identified in the first step. Each conflicting segment associates with a policy conflict and a set of conflicting rules. Also, the correlation relationships among conflicting segments are identified and conflict correlation groups are derived. Policy conflicts belonging to different conflict correlation groups can be resolved separately, thus the searching space for resolving conflicts is reduced by the correlation process[9].

4.3PROJECT DESCRIPTION

A novel anomaly management framework for firewalls based on a rule-based segmentation technique to facilitate not only more accurate anomaly detection but also effective anomaly resolution. Based on this technique, a network packet space defined by a firewall policy can be divided into a set of disjoint packet space segments. Each

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

segment associated with a unique set of firewall rules accurately indicates an overlap relation among those rules. We also introduce a flexible conflict resolution method to enable a fine grained conflict resolution with the help of several effective resolution strategies with respect to the risk assessment of protected networks and the intention of policy definition[10].

V. MODULES DESCRIPTION

Correlation of Packet Space Segment:
The major benefit of generating correlation groups for the anomaly analysis is that anomalies can be examined within each group independently, because all correlation groups are independent of each other. Especially, the searching space for reordering conflicting rules in conflict resolution can be significantly lessened and the efficiency of resolving conflicts can be greatly improved.
Action Constraint Generation:
In a firewall policy are discovered and conflict correlation groups are identified, the risk assessment for conflicts is performed. The risk levels of conflicts are in turn utilized for both automated and manual strategy selections. A basic idea of automated strategy selection is that a risk level of a conflicting segment is used to directly determine the expected action taken for the network packets in the conflicting segment. If the risk level is very high, the expected action should deny packets considering the protection of network perimeters
Rule Reordering:
The solution for conflict resolution is that all action constraints for conflicting segments can be satisfied by reordering conflicting rules. In conflicting rules in order that satisfies all action constraints, this order must be the optimal solution for the conflict resolution.
Data Package:
When conflicts in a policy are resolved, the risk value of the resolved policy should be reduced and the availability of protected network should be improved comparing with the situation prior to conflict resolution based on the threshold value data will be received in to the server.

VI. FUTURE WORK

Our future work includes usability studies to evaluate functionalities and system requirements of our policy visualization approach with subject matter experts. Also ,we would like to extend our anomaly analysis approach to handle distributed firewalls. Moreover, we would explore how our anomaly management framework and visualization approach can be applied to other types of access control policies.

VII. CONCLUSION

We have proposed a novel anomaly management framework that facilitates systematic detection and resolution of firewall policy anomalies. A rule-based segmentation mechanism and a grid-based representation technique were introduced to achieve the goal of effective and efficient anomaly analysis. In addition, we have described a proof-of-concept implementation of our anomaly management environment called FAME and demonstrated that our proposed anomaly analysis methodology is practical and helpful for system administrators to enable an assurable network management

REFERENCES

1. E. Al-Shaer and H. Hamed, “Discovery of Policy Anomalies in Distributed Firewalls,” IEEE INFOCOM ’04, vol. 4, pp. 2605-2616, 2004.
2. Udayakumar R., Khanaa V., Saravanan T., "Analysis of polarization mode dispersion in fibers and its mitigation using an optical compensation technique", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4767-4771.
3. Wool, “Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese,” IEEE Internet Computing, vol. 14, no. 4, pp. 58-65, July/Aug. 2010.
4. Bhuvaneswari B., Hari R., Vasuki R., Suguna, "Antioxidant and antihepatotoxic activities of ethanolic extract of Solanum torvum", Asian Journal of Pharmaceutical and Clinical Research, ISSN : 0974-2441, 5(S3) (2012) pp. 147-150.
5. F. Baboescu and G. Varghese, “Fast and Scalable Conflict Detection for Packet Classifiers,” Computer Networks, vol. 42, no. 6, pp. 717-735, 2003.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

6. Udayakumar R., Khanaa V., Saravanan T., "Chromatic dispersion compensation in optical fiber communication system and its simulation", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4762-4766.
7. L. Yuan, H. Chen, J. Mai, C. Chuah, Z. Su, P. Mohapatra, and C.Davis, "Fireman: A Toolkit for Firewall Modeling and Analysis,"Proc. IEEE Symp. Security and Privacy, p. 15, 2006.
8. Sathyanarayana H.P., Premkumar S., Manjula W.S., "Assessment of maximum voluntary bite force in adults with normal occlusion and different types of malocclusions", Journal of Contemporary Dental Practice, ISSN : 1526-3711, 13(4) (2012) pp.534-538.
9. J. Alfaro, N. Boulahia-Cuppens, and F. Cuppens, "Complete Analysisof Configuration Rules to Guarantee Reliable Network Security Policies," Int'l J. Information Security, vol. 7, no. 2, pp. 103- 122, 2008.
10. Udayakumar, R., Khanaa, V., Saravanan, T., "Synthesis and structural characterization of thin films of sno2 prepared by spray pyrolysis technique", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp.4754-4757.
11. T.Nalini ,A.Gayathri,HVS Based Enhanced Medical Image Fusion ,International Journal of Innovative Research in Computer and Communication Engineering,ISSN (Print) : 2320 – 9798 , pp 170-173, Vol. 1, Issue 2, April 2013.
12. S.Thirunavukkarasu, r.K.P.Kaliyamurthie ,EFFICIENT ALLOCATION OF DYNAMICRESOURCES IN A CLOUD,International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2249-2651, pp 24-29,Volume1 Issue3 Number2–Dec2011.
13. K.G.S. VENKATESAN,Planning in FARS by dynamic multipath Reconfiguration system failure recovery in Wireless Mesh Network,International Journal of Innovative Research in Computer and Communication Engineering,ISSN(Online): 2320-9801,pp 5304-5312,Vol. 2, Issue 8, August 2014.
14. G.Michael, An Empirical Approach – Distributed Mobility Management for Target Tracking in MANETs ,International Journal of Innovative Research in Computer and Communication Engineering , ISSN (Print) : 2320 – 9798 , pp 789-794 , Vol. 1, Issue 4, June 2013.
15. G.AYYAPAN , Malicious Packet Loss during Routing Misbehavior - Identification, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, pp 4610-4613 ,Vol. 2, Issue 6, June 2014