IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-5 E-ISSN: 2347-2693

Network Security and Policy Enforcement System

Nagaveni[1*], Sujata.Terdal[2]

[1]Department of Computer Science, PDA College of Engineering-VTU University, Kalaburagi, India
[2]Department of Computer Science, PDA College of Engineering, VTU University, Kalaburagi, India

[*]*Corresponding Author: nagaveni.rasure19@gmail.com, Tel.: +91-9483130770*

Online Available at www.ijcseonline.org

Received: 19/Apr/2017, Revised: 25/Apr/2017, Accepted: 24/May/2017, Published: 30/May/2017

***Abstract*—** Network operators will rely on the security services to protect the IT infrastructures. It describes design, development and implementations of organizational policies using OCS (Open Computer System) software. These policies are enforced automatically in distributed network environment. We aim to reduce human intervention by developing a practical network reconfiguration system, in that system we simply deploy security policies which are handled by the software. The main component is OCS (open computer system) which consists of different modules of SNMP(simple network management protocol) they are SNMP communities, SNMP groups, SNMP target address and SNMP users etc. Network device automated management tools contains many firewalls in dynamic environment. It is necessary to enable network elements by reconfiguring without any human intervention . The main focus of this project is OCS-NG(open computer system next generation) inventory software that contains all related information's and it is connected to workstations. Finally, the system collects the information efficiently and store the security management information in the database for off-line analysis required for network based policy enforcement.

***Keywords*—** NetworkManagement, Security, Policyspecification, Managementconsole, VLANconfiguration.

I. INTRODUCTION

A primary concepts of computer information networks is necessary to recognise the virtues of network security and policy enforcement. In computerised age, many network components are required to make large network infrastructure, network security is expanded. Network fundamentals are required to enforce the network access control policies. It is an active part of the organisation. It preserves valuable information assets. The network security issues are used in an effective way and it is used to check the performance of network. Switches application management, control the network and give economical and high quality networking services to the users. The challenge for these network elements is to know the right reconfiguration so that the appropriate security policies are upheld preventing illegitimate users from gaining access. The main aim is to maintain network security and policy enforcement; the network security can be public or private.

Elementary Information should be protected and stored which is done at the expense of adequate network security[1]. The SNMP (simple network management protocol) gather the details from devices such as routers, switches, workstations, printers etc. It maintains some standard for management of network hence providing network security using protocols.

Policy based technology is implemented to configure the policies in the distributed environment. Policy is defined as ideas or rules which perform action in the individual system and related. The primary goal is to enforce policies and provide security using OCS(open computer system). PSA(Professional service automation) is a tool which performs the similar action as that of OCS and the architecture which supports to enforce the policies is HSA (Hybrid service architecture).The result obtained from this architecture is analysis of policy enforcement efficiency.

OCS is a software that uses policy based technology, the main goal is to enforce the organisational policies. It is also an authenticating system in which all the component systems are authenticated and also it ensures returning of appropriate response to the entity that is authenticating, it may be server authentication or password authentication and related[2] , [3], [4],[9].

The main purpose is to enforce organisational policies ensuring security of network using OCS tool. There are many hardware and software devices that enforce and access control policy. Firewall provides balance and security against threats [7].

Section I contains the introduction of OCS (open computer software), Section II contain the SNMP in network security, Section III contain the system design Section IV contains related work Section V contains system architecture Section VI contains results Section VII contains conclusion and future scope.

II. SNMP IN NETWORK SECURITY

SNMP is a simple management network protocol .It is the standard way of monitoring software devices and hardware devices .There are different versions such as : SNMPv1, SNMPv2c, SNMPv3. This protocol, play a vital role in implementing security access policies by reconfiguring network devices such as switch, routers hub etc.

SNMP requires few basic components for network security and network monitoring such as:

A. Managed device
B. Agent
C. Network System Management

A. Managed device

The nodes of device administer SNMP interface and access the node specific information. It also exchanges information with NMS (Network management system). The managed device can be any hardware device such as router, switch, bridges, and hub. These managed devices acts as point of enforcement.

B. Agent

An agent is termed as a management software that resides on managed devices. This agent contains all the management information. These information's or data obtained are variables of MIB (Management information base) and ODI (Object identifier).

MIB (management information base), it is the database in which data is organised hierarchically. Most of the information is accessed by SNMP protocol. This MIB converts variables into string these string or numbers are called ODI(object identifier). Each ODI is a string that identifies an object and MIB uses the notation such as RFC 2578. These objects access the network device that we want to monitor. Thus MIB's and ODI describe the structure of policy management data. Detection and monitoring of the network devices helps to prevent the unauthorised access.

C. Network Management system(NMS)

NMS is used to monitor both software device and hardware device components in the network . It usually records the data from network device and report it to administrator. This network analysis information is required for enforcing large number of access policies. NMS ensures the network analysis of the system. The benefit is it allows the users to monitor entire network device operations using central computer. All the employees or team member can access the information or retrieve the data, it contributes in enhancing of the network security.

III. SYSTEM DESIGN

A. Existing System

This project mainly deals with enforcing the organisational policies using policy management systems. The task of the management system is to deploy and enforce the policy within no time. Network reconfigurations are made by the policy management system but there is difficulty while fetching the information from network devices. The system is maintaining the list of all the software information and hardware information manually taking more time to retrieve and delete single information. When the information are not available at the router or administration points on time it becomes difficult to enforce and access the policies.

B. Disadvantages of Existing System:

- GUI is used to express policies but they have no defined language to specify policies.
- Identification of the dispute in expressing the policy is more difficult.

C. Proposed System

We propose the model or the system to enforce the policies that it should be implemented by the management system for achieving all the objectives. We develop the system as the result it has to obtain the policy and deploy without any disputes. Proposed system is designed by keeping minute details in mind either it is administration, analysis or for commercial use. Policies are specified and enforced using enforcement points. Proposed system is automated, and it deploys the organisational based policies.

For enforcing policies we need actual policy enforcement device, this model propose the network infrastructure that supports the service to implement these policies. VLAN configurations via switches support to deploy the policies. The policy data are embedded in an active directory from which data are accessed and implemented.

D. Advantages of Proposed System:

- Provides best services to the user by configuration of the network devices.

- It is less dependent on the system manager making the system highly intelligent.

IV. RELATED WORK

Network security consists of policies to prevent unauthorised access. Related work describes about policy network system management and network policies administration. The system architecture consists of routers [1] it recognises users and their managed devices. Router gives matching routing table of nodes to enforce policies using shortest path. For policy security management, we need authenticated system. It uses authentication techniques(text passwords, Visual passwords and graphical passwords) [2] to authenticate all the components. It is old method to remember character but the new method is to remember the images. Graphical method is more secure then text and visual password method. Password authentication technique [3] is used to provide security to the password. This authentication technique is for customer application, it has reliability and cost drawbacks. Designing authentication techniques require authentication protocols. The authentication protocol[4] designer includes the application of public and secret key algorithms that describes about assurance and performance level of authentication. For network authentication we can deploy network control admission systems[5] . This system contains NAC managers and servers , it is an enforcement parameter. Policy based approaches to the NAC systems are very important, the rules enforced in the system management, governs the behaviour of the system. Policy refinement[6] is process of converting high level policy statement into low-level. It translates high-level policies into operational policies that system can enforce. It gives techniques of policy analysis. There are different kind of policies to be enforced such as principal policy , directional policy, organisational policy and functional policy . In the network hierarchy[7] of all these different types are defined in a high level management plane. The main reason to consider security is to protect all the information of the device[8]. Authentication is required for security purpose authentication provides confidentiality [9] and it can be maintained to the large extent. For e-commerce, the firewall security is very important; internet and personal computer are isolated. These are hardware devices and software devices that enforce and access policies between network. Security of the software[10] is just one quality attribute in distributed system. This is helpful in enforcing number organisational policies.

V. SYSTEM ARCHITECTURE

Policy established system management is the network system which is accomplished based on policies. Policy is the collection of ideas or rules and services, each policy rule is defined by a collected set of conditions and set of actions. In these days network systems are implemented in the large scale. It makes convenient to use rules. Policy provides dynamically changing management strategies.

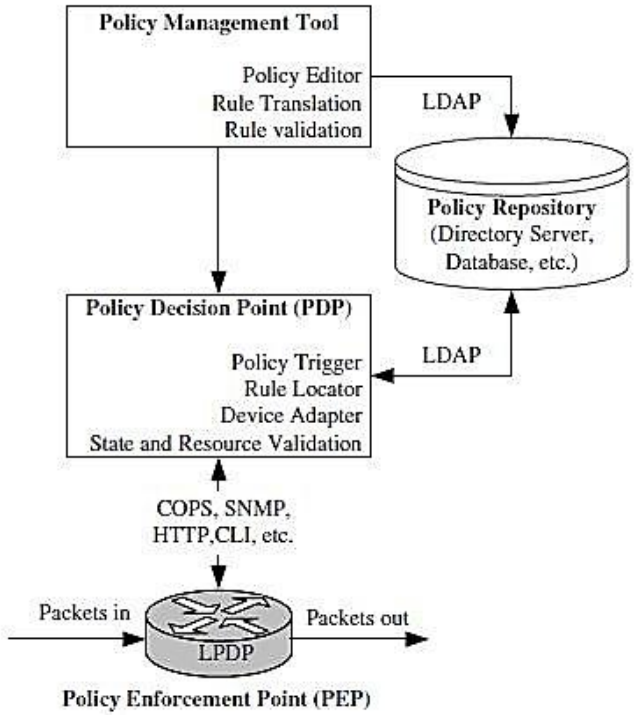

Figure 1. Enforcement of policies

Enforcement of policies in the figure above, is the policy enforcement network architecture it includes following components:

A. Management Tool
B. Policy Repository
C. Point for policy enforcement

A. Management Tool

Management tool is an administrative tool or host. This software helps for Policy Editing, Rule Translating and Rule Validation. In Policy Editing administrator, it can change the policy such as policy name and setting etc. Rule conversion means a marked changes, it moves at every point in the figure with the equal distance and same directions. Rule Validation is similar to data validation which is validated after policy has been successfully enforced.

B. Policy Repository

Policy Repository is the data storage area for policy information. These data can be application specific or operating system specific. It can reserve information, rule locator, device adapter etc

C. Points for policy enforcement

It is the information device such as router, switch, and hub. The policies are enforced or implemented as directed by point of devices for policy decision. The policies are enforced by dynamic configuration changes made in access control list(ACL).ACL defines the justice to make provision or oppose or audited. Label distribution protocol (LDP) is a procedure from which routers are capable of exchanging mapping label information's. Open Policy Services Protocol is proposed to exchange network information policies and the network policy decision points. On booting management information systems they report their capabilities to the policy server through service protocol. Command line interfaces (CLI). we can use CLI for particular application to take standard actions on large number of network objects.

VI. RESULTS

The policy enforcement efficiency analysis are made using PSA(Professional Services Automation Tool) and HSA (Hybrid Security architecture). The graph analysis has two components Number of rules in x-axis and number of elements in y-axis. There are 3 real policies employed with high efficiency as explained in fig 2 using tool and architectural design.

A. Experimental Environment

The number of the network access nodes and IP segment may be aggregated if there are many access nodes. This application is calculated according to each real policies they are enforced and shadowed by high-priority one.

Professional automation tools are implemented using java frameworks. It is the policy enforcement tool. This experiment is conducted on single Intel i7 and memory is 3.4 GHz CPU work station. According to this experiment three real policies are employed in the analysis and other policies are generated using its default arguments. This result briefly gives the idea of real policy enforcement obtained on x-axis(number of rules) and Y-axis(number of elements) using automation tool and hybrid architecture.

HAS (Hybrid Security Architecture) is the network hybrid architecture form. It is a design that decouples security services from routing and allows the integration of hardware and the software. The above analysis compares the memory efficiency of HSA and PSA. The 100-scale policies of different types are enforced. It is observed that HAS fails to continue in the analysis while PSA works on all the policies producing evolution results.

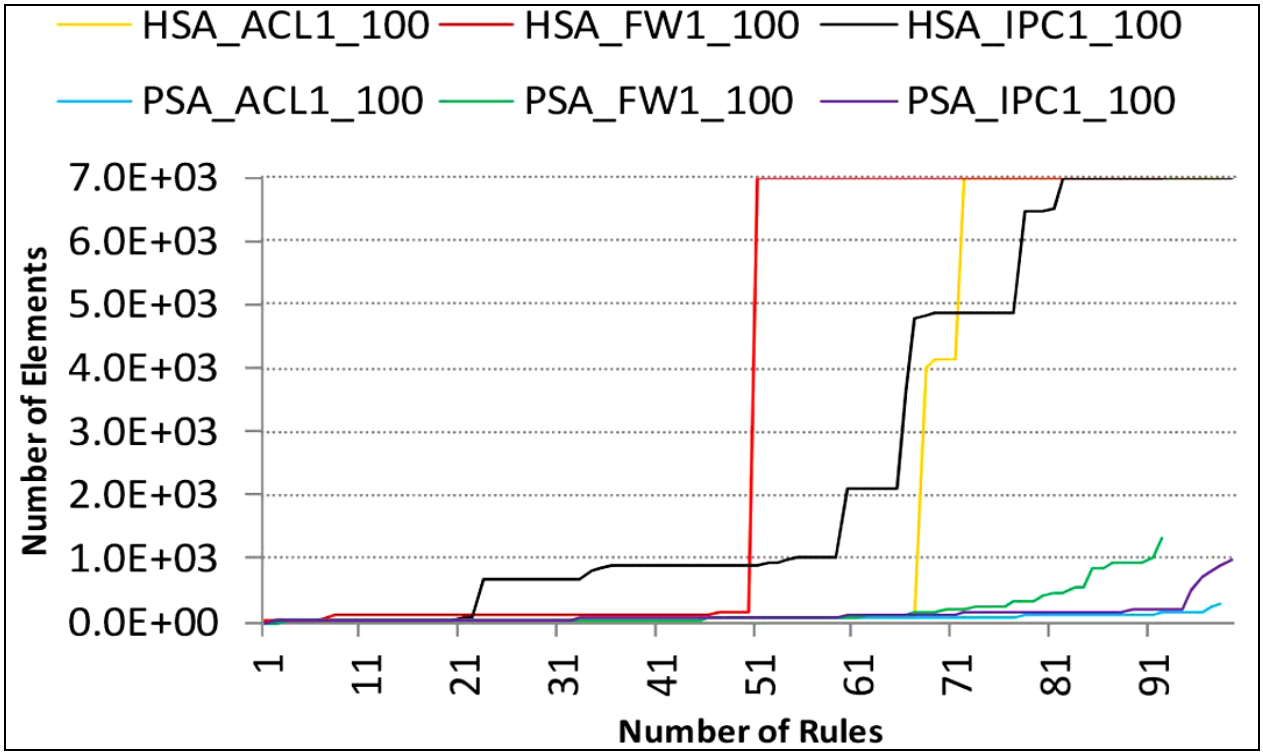

Figure.1: Policy Enforcement Efficiency

VII. CONCLUSION AND FUTURE SCOPE

Policy enforcement and management networks is of great use within academics, business and researchers . It provide higher stability for management operation regarding the translation of specific policy rules. Here we identify the components that are implemented in the creation and enforcement of the policies. We could make an appropriate construction of the policies and enforce them. There is an effective interactions between administration points and the protocols which helped them to enforce dynamically. Policies are created and implemented at different levels within the management plane. The important point of the results is the procedure for enforcing the policies in the system architecture. TCP/IP switches and routers used in this architecture are directly controlled by using this OCS software tool. We proposed graphical user interface that makes system admin to identify and validate the policy. Other than validation the interface also supports implementation details. The long term goal of this project is the creation of organizational policies from the management tool and effectively implementing with the organisation. When the enforcement of policies are completed the policy validations are handled by testing each component so that management tool become scalable.

For the future plane we have to implements policies using SNMP agent including all the features defined in RFC 1213 management protocols and RFC 2863 it is used for management purpose. This modules will be proposed to reconfigure the string variable stated in MIBs. The GUI makes the administrator to reconfigure and manage network parameters by using strategy policies. MIB's provide database to network related scenario maintaining a unique platform.

REFERENCES

[1] Eld G., Hundley K., "*Cisco Security Architectures*", McGraw-Hill, New York, pp.1-635, 1999 .

[2] S Gkarafli, AA Economides, "*Comparing the proof by knowledge Authentication Techniques*", international Journal of Computer Science and Security (IJCSS), Vol.4, Issue.2, pp.37-55, 2011.

[3] R. Morris, K. Thompson, " *Password security*: *A case history*", Comm. ACM, Vol.22, no. 11, pp. 594-597, 1979.

[4] Harbittr A., Menasce D.A., " *A methodology for Analyzing the Performance of Authentication Protocols"*, ACM, Vol 5, no 4, pp.58-91, 2002.

[5] R. Yavatkar, D. Pendarakis, R. Guerin, " *A Framework for policy based admission control*", IETF, USA, pp.1-20, 2000.

[6] A. Bandara, E. Lupu, J. Moffet, A.,Russo, "*A goal-based approach to policy refinement*", In Proceedings of 5th IEEE Workshop on policies for Distributed system and networks(Policy 2004), NewYork,USA, pp.23-28, 2004.

[7] R. Wie. "*Policies in Network and Systems Management - Formal definition and architecture"*. Journal of Systems and Network Management Vol.2, no.1, pp.63-83, 1994.

[8] Alabady S., " *Design and Implimentation of a Network Security Model using Static VLAN and AAA Server*," In proceeding International Conference on Information & Communication Technologies: from Theory to Applications, US, pp.1-9, 2008.

[9] B.L. Riddle, M.S. Miron, J.A. Semo, "*Passwords in use in a university timesharing environment*", Computer and Security, Vol. 8, no.7, pp. 569-579, 1989.

[10] Gholamreza Shahmohammadi, "*Scenario-based Evaluation of software Architecture styles from the security viewpoint*", international Journal of Computer Science and Engineering (IJCSE), Vol.4, Issue.4, pp.10-20, 2016 .

