Quest Journals
Journal of Electronics and Communication Engineering Research
Volume 2 ~ Issue 8 (2014) pp: 01-04
ISSN(Online) : 2321-5941
www.questjournals.org

Research Paper

Network Visibility As Key Measure To Network Management

Neyole Misiko Jacob[1]
[1]*Lecturer. Jomo Kenyatta University of Agriculture and Technology Kitale Campus, Kitale town, Kenya.*

Received 11 November, 2014; **A**ccepted 06 December, 2014 © The author(s) 2014. Published with open access at **www.questjournals.org**

ABSTRACT:- *Network management may be explained as the administration of large scale computer and telecommunications networks at the top level and the execution of the set functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the network resources including performing functions such as initial network planning, frequency allocation, predetermined traffic routing to support load balancing and cryptographic key distribution authorization among other measures. The knowledge of exactly what happens in a given internal network is usually a top priority. Total visibility allows for better security planning to prevent and neutralize emerging threats and to spend more efficiently on information technology resources. Also allows one to maintain a smaller, more focused IT team to manage the ever increasing complexities of internal networks and the activity of users who occupying them. Most network administrators try resolving network problems from a point of no know-how. The basic approach one can put in place to ensure that an organization network is manageable is to make the internal process and transmissions within the network visible for better administration. This paper brings to light the importance of network visibility to an organization by focusing on dangers network administrators ignore and this motivation of the study would help on adding measures to protect and manage organization network by network administrators.*

KEYWORDS:- *Network Visibility, QoS, Network Resources,*

I. INTRODUCTION

Network management may be explained as the administration of large scale computer and telecommunications networks at the top level. It is the execution of the set functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the network resources including performing functions such as initial network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, security management, performance management, bandwidth management and accounting management.

The knowledge of exactly what happens in a given internal network is usually a top priority. Total visibility allows for better security planning to prevent and neutralize emerging threats and to spend more efficiently on information technology resources. Total network visibility, allows one to maintain a smaller, more focused IT team to manage the ever increasing complexities of internal networks and the activity of users who occupying them. Most network administrators try resolving network problems from a point of no know-how. The basic approach one can put in place to ensure that an organization network is manageable is to make the internal process and transmissions within the network visible for better administration.

II. BACKGROUND

Network visibility can be define as a measure of the ability of a protocol to precisely localize network failure causes. The visibility 'V', of a protocol can be defined as the difference between the total number of failure causes in its layer and the number of failure causes that the protocol cannot identify precisely. For instance, if a network layer protocol can correctly identify the failure cause due to reboots and Ingress Drops but cannot identify any of the 4 other causes listed in the dictionary [1] for network protocols, then for this protocol, v = 6 – 4.

Protocols try to enhance visibility by including additional bits in packet formats, for instance a protocol might add an end-to-end flag bit to indicate that a packet dropped due to congestion. Such an addition comes at

the expense of energy spent on transmission of that extra bit. The combination of the energy and the visibility metric provide a protocol designer with trade-off choices for designing efficient and visible protocols. [2]

There are six identified major areas that ensure network visibility particularly using Cisco IOS Net Flow Data, these are; identifying applications on your network, finding top talkers on your network, investigating threshold exceptions, validating QoS implementations, compare application usage patterns and understanding bandwidth utilization and growth.[3]

Santos, [4] indicated that the first step in the process of preparing ones network and the staff to successfully identify security threats was by achieving complete network visibility. This level of network visibility can be achieved through existing features on network devices that are already available. Additionally, one should create strategic network diagrams to clearly illustrate the packet flows and where, within the network this may provide security mechanisms to identify, classify, and mitigate the threat.

Much emphasis for today's intrusion detection systems (IDSs) focus on a particular type of monitoring data such as host logs or network packets rather than synthesizing a broader view across multiple sources like the keystrokes as seen on a host, past DNS lookups, honeypot data, internal Net-Flow records, correlations between network activity and local desktop input or lack thereof.[5]

The response to attacks on the other hand entails not only real-time detection but also, the post facto forensics. Operators may answer crucial questions about the scope of an intrusion and the breadth of possible damage by drawing upon high-quality logs of past activity. Storing disparate forms of information in a unified fashion can not only save operators time in finding the answers to their questions, but also renders the process less erroneous.

THE MISSING GAP

The theory above leaves out the role of the network administrator who should be given attention in terms of training and network affairs awareness. This also applies to the physical architecture of the network. Most networks are not clearly structured and therefore solving problems or managing such networks becomes a burden or impossible to the administrators.

The visibility of a network cannot be addressed by a single line of command or mouse click but it will involve a lot of effort. Some of that effort will include vetting of all devices that connect to your network whether physically or remotely. This is important because these same devices, especially those that are personal can be used as loopholes or targets by hackers to infiltrate your network.

PROBLEM DEFINITION

Lack of intelligent apparatus and effective mechanisms to aid in management of the organization's network poses many challenges that extend to various departments in an organization. This is particularly evident in the threats that are encountered and many others that go unnoticed but always leave some scars on an organization day-to-day running of its operations. For an organization to achieve the desired goals and be able to deal with the network administration problems, it has to ensure that all the challenges and needs that the network it uses are identified. Some of these needs may include, security, Quality of Service (QoS), high speeds, among others. When these needs are identified then they can be used as a platform to design a program that addresses those requirements**.**

III. OBJECTIVES OF THE STUDY

The general objective to the study was to identify problems that organization face as far as management and administration of the network is concerned and henceforth suggest ways that network visibility can be used to enhance the efficiency, security and effectiveness of the network.

The study also aimed to identify areas that require attention with regards to an organization network management giving recommendations on what needs to be done accordingly. It went ahead to identify measures put in place to secure networks within organization.

IV. RELATED STUDIES

According to Manage Engine publication [6] Network visibility, to put in the simplest way, is to have an awareness of the various applications and conversation traversing the network, be it LAN or WAN. To be

aware is to be able to control the network activities. Network visibility also helps in allotting optimum bandwidth to the business critical applications.

Taking Cisco as a simulated example, Cisco Application Visibility and Control (AVC) provides a powerful pervasive, integrated service management solution based on stateful deep packet inspection (DPI). With the Cisco AVC, instead of processing packets as individual events the Cisco ASR 1000 Aggregation Services Router fully reconstructs flows and the Layer 7 state of each application flow for application- and session-based classification and management of IP traffic. [7]

With this CISCO shows that millions of users worldwide connecting to an array of media from many sources, enterprises and service providers have not been able to accurately and completely monitor, report on, and manage service and performance levels of all of these services. To reduce network congestion and increase operational efficiency and overall profits.

Through network visibility one is able to understand the value of network recording, which in turn is important to understand the types of threats to the network. The types of issues that can impact an enterprise's network and its performance may include: Security-Related Threats, Network Performance Issues and Application Performance Issues among other issues. [8]

Paloalto[9] networks indicates that Port numbers, protocols, and IP addresses are useful for network devices, but they tell one nothing about what is on the network. Detailed information about the applications, users, and content traversing ones network empowers them to quickly determine any risks they pose and quickly respond.

According to the Impact of Cost Effective Network Visibility on the Profitability of your Financial Institution white paper [10] which states that with all the money being spent on servers, virtualization, storage, security and high-speed links; it is difficult to justify the expense of monitoring, time stamping and performance tuning tools that one needs to tune your network and to provide audit trails. Yet if one does not have this visibility into his/her network, he/she knows that he's/she's operating blind - blind to attacks going to bandwidth choke points, blind to network performance problems, blind to fraud and blind to security breaches. This lack of visibility increases as some of they consider moving noncritical services and storage to private or even public clouds.

As mobile operators [11] transition their legacy networks to 4G LTE to provide better services for their customers, they face new and significant operational and cost challenges. The Brocade Network Visibility solution helps operators extract key insights from their networks to make intelligent, real-time business decisions, simplifying the migration to the next-generation network.

ISO requirement on network administration and management

ISO/IEC 27001:2005, part of the growing ISO/IEC 27000 family of standards, is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). ISO/IEC 27001:2005 formally specifies a management system intended to bring information security under explicit management control. [12]

The Standard of Good Practice for Information Security, published by the Information Security Forum (ISF), is a business-focused, practical and comprehensive guide to identifying and managing information security risks in organizations and their supply chains. The recently published 2011 Standard is the most significant update of the standard for four years. It includes information security 'hot topics' such as consumer devices, critical infrastructure, cybercrime attacks, office equipment, spreadsheets and databases and cloud computing.

The 2011 Standard is aligned with the requirements for an Information Security Management System (ISMS) set out in ISO/IEC 27000-seriesstandards, and provides wider and deeper coverage of ISO/IEC 27002 control topics, as well as cloud computing, information leakage, consumer devices and security governance. In addition to providing a tool to enable ISO 27001 certification, the 2011 Standard provides full coverage of COBIT v4 topics, and offers substantial alignment with other relevant standards and legislation such as PCI DSS and the Sarbanes Oxley Act, to enable compliance with these standards too.[13]

V. SOLUTION

The study suggested that proper network administration and management involve purchasing of applications like Network monitoring and performance management software, IDS (Intrusion Detection Systems), Antivirus programs with malware and anti-spyware features among requirements. It also suggested that devices were also necessary to complement the application side.

There was need to train competent network administrator who are able to handle issues related to network management and maintenance. This persons must ensure that they are well updated with the current

changes not only in the local area networks but also be aware of the new trends in the networking field. The network administrators therefore have to ensure that they carry out real time statistics and long-term analysis on the networks they manage. Depending on the magnitude of the network, they are expected to ensure that these operations are analysed as soon as possible and that recommendations are done without delays.

Along these they should also carry out threshold monitoring which involve measuring the performance of the devices on the network based on a set threshold and when it is not reached, they should be indicators or triggers which send information to them to resolve such issues. In addition, any new networks must involve a comprehensive network planning that takes care of all needs instead of trying to resolve them when they have caused problems this reduces huge financial implications as well as securing organization data.

VI. RECOMMENDATIONS

There is much that needs to be done before the organization makes the first leap into a more visible and manageable network. One of the fundamental jobs of a network administrator is networking monitoring. Networking monitoring is the process of checking the computers, systems, and services that comprise a network. This examination allows a network administrator to maintain a robust network and even to improve upon the network. You never know when a power supply is going to burn out, when a server is going to crash, when network bandwidth drops or when the LAN is hacked.

However, even though one does not know when poor network events will occur, he/she can be prepared for them. Effective networking monitoring will alert one the moment that a situation arises for quick and immediate response so as to minimize down-time. While a networking monitoring systems can provide information about problems, it can also provide information about improving the network. A good system will allow one to generate log files and performance charts that detail the system's capabilities and responses. With this data, the administrator can tweak settings to find the optimal set-up.

Some of other areas that have to be addressed include; improving the policies to incorporate the new system and all its dimensions, ensure that the applications that they buy are effective in addressing the visibility in the network. These improvements should not become hindrances to the system, instead they should enhance its performance.

They must also ensure occasional audits of the network in addition to the frequent analysis for better understanding of the whole network performance. Measures such as ; Alerting, performance monitoring, database monitoring, network & system monitoring, service level monitoring, network traffic monitoring, protocol analysing & packet capturing, SNMP & VoIP monitoring, as well as environmental monitoring among others.

REFERENCES

[1]. The communications protocol dictionary http://www.thefreedictionary.com/Networking+protocol
[2]. Vasseur J. P & Dunkers. A (2010) Interconnecting Smart Objects with IP The Next Internet. Elsevier Inc.30 Corporate Drive, Suite 400, Burlington, MA 01803, USA.
[3]. Mao G., Brian D. O. Anderson and Baris Fidan, "Path loss exponent estimation for wireless sensor network localization", Computer Networks, vol. 51, no. 10, pp. 2467-2483, October 2007.
[4]. Omar Santos (2008). "Identifying and Classifying Network Security Threats" Cisco Press. Pearson Education, 800 East 96th Street, Indianapolis, Indiana 46240 http://www.ciscopress.com/articles/article.asp?p=791595
[5]. Mark. A, Christian. K, Vern. P, Robin. S, Nicholas. W (2008) Principles for Developing Comprehensive Network Visibility Ross Moore, Mathematics Department, Macquarie University, Sydney. Manage Engine http://www.manageengine.com/
[6]. CISCO (2012) Cisco Visual Networking Index: Forecast and Methodology, 2011–2016 White Paper. Americas Headquarters Cisco Systems.Inc. San Jose, CA. https://www.google.com/?gws_rd=ssl#q=cisco+2011+p
[7]. Frost and Sullivan (2013) "Interactive Intelligence" accessed at http://www.inin.com/resources/ProductLiterature/Frost-and-Sullivan-Cloud-based-Contact-Center- Award.pdf
[8]. Palo Alto Features (2014) Application Visibility. Palo Alto Firewall accessed at http://www.paloalto-firewalls.com/features-2/
[9]. Gigamon- Impact of Cost Effective Network Visibility on the Profitability of your Financial Institution: http://www.gigamon.com/stuff/contentmgr/files/1/4e0440388067b22fec536e3275ddac1c/download/financial_wp_web.pdf
[10]. Brocade http://www.brocade.com/solutions-technology/service-provider/network-visibility/index.page Wikipedia http://en.wikipedia.org/wiki/ISO/IEC_27001:200
[11]. Wikipedia http://en.wikipedia.org/wiki/Standard_of_Good_Practice
[12]. http://www.informit.com/articles/article.aspx?p=791595
[13]. http://www.monitortools.com/
[14]. http://www.networkperformancedaily.com/2007/07/netflow_monitoring_six_tips_fo.html
[15]. http://www.reuters.com/article/pressRelease/idUS157326+08-Jan-2008+BW20080108