ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 6, Issue 1, January 2017

Security monitoring and Management of Traffic Performance in Converged Networks

Shaikh Abdul Azeem, Dr. Satyendra Kumar Sharma,

***Abstract*— carrying traditional business application data (e.g., email and file transfer), internal networks are now also carrying voice traffic and on demand video. Coupled with additional alerting and control traffic like NetBIOS and SNMP, this is creating a perfect storm of monitoring and security problems for information security and network engineering professionals.**

Universally major network engineers have incorporated network convergence into their strategy to grow service revenues and minimize actual capital and operating costs Convergence occurs in applications, in network control, in the higher transport layer, as well as in the access network. This convergence of networks means that various types of traffic flows, which have been carried by separate specialized networks, now share the resources of a single IP-based network. In the access, the trends are towards wireless convergence as well as convergence of various wireless access technologies.

***Index Terms*— convergent, divergent, converged networks**

INTRODUCTION

"The new initiatives of the 21st century are based on the business process transformation within a service-oriented architecture, "says Frank Dzubeck in a Feb. 2008 Network World article about the growing threat of network latency. "Add organizational and supply-chain transformation through VoIP, video-based collaboration, and innovative real-time, industry-specific applications, and we have a major festering problem."1 Performance and security monitoring are growing closer together than ever as these new and traditional forms of traffic clog our networks. Although the presence of a performance or security issue does not necessarily indicate the existence of the other, many analysts are realizing the benefits of behavioural baselines and how a more holistic approach can alleviate the problems of both congestion and security. For example, large data transfers that are causing congestion issues could potentially indicate an attacker retrieving database records. Another major concern for today's analysts is the fine-tuning of technologies that communicate over the network. Every SNMP-capable device can be configured to send alerts only for very specific events and conditions. With proper tuning, intrusion detection systems can have false positives identified and removed, and other devices and applications can be similarly con- figured to prioritize alert data.

Network convergence refers to the provision of telephone, video and data communication services within a single network. In other words, one pipe is used to deliver all forms of communication services. The process of Network Convergence is primarily driven by development of technology and demand. One main goal of such integration is to deliver better services and lower prices to consumers. Users are able to access a wider range of services, choose among more service providers. On the other hand, convergence allows service providers to adopt new business models, offer innovative services, and enter new markets.

I. NEED OF CONVERGED NETWORK

The critical drivers that lead an organization to consider a converged network are the measurable cost savings related to infrastructure, staffing and facilities, as well as improvements in productivity and customer care. There are certain circumstances that can accelerate the evaluation and adoption process

- Building a new office or moving to a new location.
- End of lease for PBX or support contract.
- Necessary upgrades for data network.
- Lack of expansion capacity of current voice network.

II. NETWORK MONITORING

- **Voice over IP (VoIP)**

VoIP makes use of a number of new protocols. The two that are most commonly used are H.323 and the Session Initiation Protocol (SIP). There are also several others that are commonly encountered on converged networks, some of which are proprietary, for example Cisco's Skinny Client Control Protocol (SCCP).

- **Video**

Because video is increasingly being used for training and other corporate purposes, many networks are now carrying video over IP in addition to voice and traditional data. The Real-time Transport Protocol (RTP) is often used for transmission of video data within IP, as

are other protocols like Real-Time Streaming Protocol (RTSP) and Real Networks' Real Data Transport (RDT).

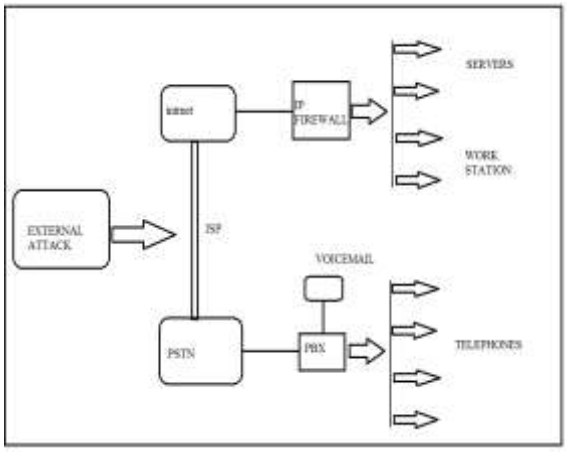
III. OBJECTIVES OF THE RESEARCH:

1. To study the converge network.
2. To monitor the security in the network
3. Analysis over the converge network
4. Provide solution to the available problems.

IV. SECURITY AND PERFORMANCE IMPACTS ON CONVERGED NETWORKS

➢ **Performance**

Circuit-switched networks have also traditionally been known for stability and reliability, with industry standards of 99.999% uptime considered normal. Packet-switched networks were not designed to have this level of reliability, and so extensive monitoring features and methods have been developed to attempt to rapidly detect and repair any problems. Many of these technologies are vendor-specific and don't natively interact with other tools like security monitoring and management systems. Frequently, one or several groups within an organization will use one set of tools to analyse certain aspects of the network, such as Network Operations Centre teams using SNMP tools to monitor network performance and events. Meanwhile, other groups will use entirely different tools to analyse the same network traffic for security analysis and application troubleshooting. Traditional network analysers can be used to good effect on network teams in assessing common converged network performance issues such as latency, jitter (signal fluctuation),and packet loss. With the influx of new and more complex protocols, as well as large numbers of distinct endpoints for which available bandwidth must be managed for critical services such as customer facing applications and daily business traffic, performance monitoring on converged networks is of paramount importance. For services like VoIP, the use of Quality-of-Service (QoS) mechanisms is common for dynamically monitoring and detecting common issues like latency and jitter. In most cases, high-end network equipment can be tuned to self-adjust for many issues. However, the need to continuously monitor critical services is even more pronounced in converged environments. A viable threat to VoIP is Denial of Service (DoS) attacks, which could cripple all telephone service without proper monitoring because each group is only getting some of the information but not enough to see the entire picture. For example, the network engineering team may be monitoring SNMP traps and QoS on several network segments — and may have a fair idea of what the bandwidth patterns should look like in the context of a normal behavioural baseline. However, the References information security team may have completely different views of the bandwidth usage patterns due to network forensics and event monitoring that they are performing. Without collaborating or correlating the data, significant security issues may be missed. Security teams must also keep pace with new attacks on protocols, such as SIP, which include registration hijacking and eavesdropping. Increased visibility into network traffic and behavioural baselines is critical to detect and prevent such attacks. Another major concern for security teams is the increased storage needs required in converged environments. With new critical applications and data types, the need for considerable enhancements to logging infrastructures is quickly becoming a reality. Security and audit teams are also tasked with implementing controls for regulatory and industry-specific compliance mandates, which bolsters the need for logging, forensics, encryption or other access controls.



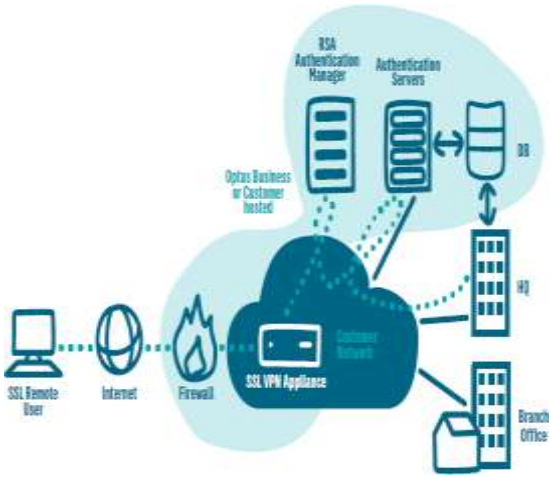
➢ **secure Service and Maintenance Access**

➢ Security

A. The lack of coordination with tools and techniques for examining converged network traffic is a real problem

Secure remote access for network monitoring and maintenance is an essential part of maintaining network and application security. The capability to automatically detect and correct equipment problems is a key step in addressing

potential security violations. A secure access approach that provides the strongest authentication means, such as one-time passwords and challenge and response techniques, for granting access to specific equipment and applications within the perimeter is necessary for services and maintenance. Using strong authentication is particularly important in this area since maintenance personnel require access to many sensitive resources of a system. Avaya's remote service and maintenance solutions have consistently had high security as an important customer need. Traditional access is via a private line modem in which access is obtained only after successful challenge and response authentication takes place using one-time passwords. The future of remote services, as with many aspects of technology, is via the Internet. As such, Avaya has developed the sophisticated Avaya™ Secure Services Gateway (SSG) that includes a firewall/VPN solution that is customer controlled. This new high-speed solution provides customers the capability to control access to their network perimeter and enforce the customer's own security policy.xix Figure 4 provides an illustration of services access through the SSG. Remote servicing personnel are challenged by the SSG platform before being granted access to service equipment on the customer premises.



Secure Remote Access for Servicing

CONCLUSION

Today, many organizations that run voice, video, and data application on the same infrastructure are implementing or moving toward converged networks. Although this often makes excellent business sense, the increase in new protocols, diverse endpoints, and overall traffic volume make network performance and security monitoring more difficult — and also more critical than ever before. Performance issues can cripple the ability to perform normal business functions, while security problems are more difficult to identify inside all these new types and patterns of traffic. New tools must address these issues by converging themselves.

Studied The Converge Network And Its Security.

REFERENCES

[1] Third Generation Partnership Project (3GPP) at http://www.3gpp.org/ 3GPP Technical Specification Group Services and System Aspects; Network Sharing; Architecture and Functional Description. 3GPP TS 23.251, Sep. 2011.
[2] 3GPP System Architecture Working Group 1 (SA1): RAN Sharing Enhancements Study Item at http://www.3gpp.org/ftp/Specs/html-info/WiSpec540028.htm
[3] 3GPP System Architecture Working Group 1 (SA1), Use case for On-demand Automated Capacity Brokering, S1-124050, November, 2012.
[4] 3GPP TSG-RAN Workshop on Release 12 and onward, Future Radio on 3GPP, June 2012.
[5] Technical Specification Group Radio Access Network; Scenarios and Requirements for Small Cell Enhancements for E-UTRA. 3GPP TR 36.932, Dec. 2012. . IEEE 802 Working Group 11 at http://www.ieee802.org/11/
[6] G. Hiertz et al. The 802.11 Universe. IEEE Communications Magazine, January 2010.

First Author research scholar, department of computer science, pacific academy of higher education &research university, Udaipur, Rajasthan, India.

Second Author Dean, faculty of engineering, department of computer science, pacific academy of higher education &research university, Udaipur, Rajasthan, India.