Importance of Providing Integrated Network Operating Centre (iNOC) for Government in Today's Technology Driven World

Sarbjeet Singh and Lokesh Dwivedi***

Abstract

The internet usage has grown at an enormous rate over the past few years, and it has almost certainly affected the lives of most people who use computers and electronic smart processing gazettes. Network security has become more important to internet users (personal computer users), organizations and the Government. It becomes important for the Government as well as private organizations to implement systems like integrated Network Operation Centre(iNOC) for the sake of security and protection of confidential information. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. iNOCis a physical location to control the operations of computer networks. iNOC's are responsible for monitoring and controlling critical services, threats, alarms, errors, and even power issues in critical networks. The range of the study will encompass the importance of the iNOC and its applications that where this concept is being implemented and with the increased use of technology what will the relevance of using such kind of systems in the Government which are providing information and communication technology infrastructure. Need of the constant monitoring of the network devices and handling their troubleshooting became the topmost priority of the organizations and the relevance of the iNOC could better be understood in today's world.

Keywords: - Network Security; Monitoring; Computer Network

* Senior Technical Director (Scientist - 'F'), Scientist - 'B', National Informatics Centre

** Department of Electronics & Information Technology, Ministry of Communications & Information Technology, Punjab State Unit, Chandigarh

1. Introduction

The internet connectivity/usage/requirement has grown at an enormous rate over the past few years, and it has almost certainly affected the lives of most people who use computers and electronic smart processing gazettes. In the past few years internet has evolved from a platform for publishing "online brochures" to an entire architecture for developing dynamic, distributed applications and services.

After continuous and widespread use of Network system in several area by the Government it's became essential to monitor, follow-up and maintain these networks to provide the best performance & efficiency for all users, so that the iNOC concept is established.

An integrated network operations center (iNOC) is a place from which administrators supervise, monitor and manage/maintain a computer network. Large enterprises with large networks as well as large network service providers typically have an integrated network operations center, a room containing visualizations of the network or networks that are being monitored, workstations at which the detailed status of the network can be seen, and the necessary software to manage the networks.

1.1 History of iNOC

The early Version of iNOC have been around since the 1960's a network control center was opened in New York by AT&T that used status boards to display switch and route information in real-time from the most important toll switches and this center developed till they got the current NOC facility concept.

In 2008 the internal network division in I.C.T center of University of Toronto established the installation process of central network infrastructure. Its main purposes was providing 24/7 high speed internet & intranet services to all university's formations. Since that time the internal network division played an Internet Service Provider (ISP) role for the University of Technology. And it became responsible for configuring, maintaining, monitoring and upgrading the network to provide high performance network and high quality services. The University of Toronto networks started with 4Mbps internet bandwidth and increased till it's get to 45Mbps internet bandwidth currently.

Devices remotely and it can check or configure many options such as:

- Maximum round-trip time.
- Changing channel width and frequencies of Access points & stations.

- Checking CCQ values for the stations.
- Checking wireless registration table.
- Changing Data rates for Access points and clients.
- Controlling connect list, access list.
- Controlling PPPoE server, PPPoE clients.
- Controlling Queue and bandwidth limits.
- Managing Firewall, Mangle, etc.
- Web proxy

2. Challenges to network security

Network security is more challenging than ever as today's Government networks become increasingly complex. With endpoints/nodes multiplying daily, and cloud computing leading to a far more dispersed application environment, the tidy north-south traffic of yesteryear is fast giving way to an east-west quagmire.

1. **State-sponsored espionage:** This challenge highlights the need to protect critical data from politically or financially motivated threats. Critical data includes the information needed to run network attached infrastructure as well as the intellectual property used to manage business and drive innovative solutions.

2. **Distributed denial of service (DDoS) attacks:** Security professionals in the financial services industry are likely to agree to our second challenge: DDoS attacks. We can expect to see a higher risk of business impacting threats with the shift from computer-based attacks, generating large number of lower bandwidth events, to virtual server or cloud-based attacks, generating ultra-high bandwidth events.

3. **Cloud migration**: The challenge is that cloud security processes and solutions are still being developed. Ultimately, with innovation and planning, cloud services could reduce business risks by providing greater flexibility, resiliency and security.

4. **Password Management:** Our challenge is putting in place and enforcing stronger user-controlled passwords that are less likely to be broken. This educational and administrative challenge requires creative solutions and enforced policies. Or, we can look at alternatives to traditional passwords, such as the use of a

federated ID.

5. **Sabotage**: Sabotage of computer networks can affect critical infrastructure and ultimately impact corporate and backbone networks. This challenge is so potentially perverse because it combines social engineering with software based tools to provide a complex multi-vectored attack profile.

6. **Botnets**: Botnets are everywhere. The challenge is that many botnet owners design systems that are more adaptive and redundant than many corporate and Government networks. Controlling this agile attack vector before it can be used as an advanced persistent threat (APT) and migrates into smart mobile devices is crucial.

7. **Insider threat**: A dissatisfied employee base provides a vector for insider security events, while the inadvertent injection of malware through removable media or web interconnections can make any employee the origination point for a network security violation.

8. **Mobility**: Management and security of mobile networks and smart mobile devices becomes even more challenging when employees want to use their own devices for business purposes. The bring-your-own-device trend exasperates this challenge when we look at protecting the critical information needed to manage the organization and the network without sacrificing the privacy of employee's personal information and activities.

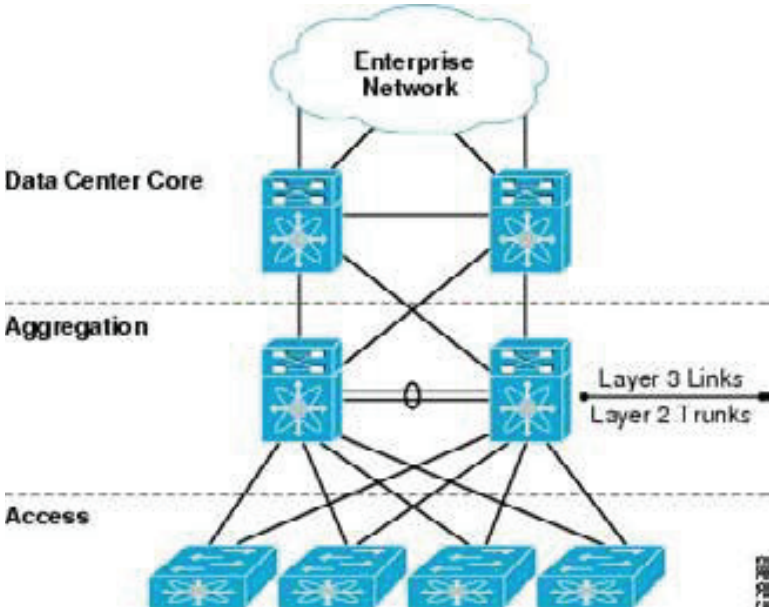
9. **Internet:** One of the greatest challenges to security professionals is the perception that the internet, a best effort network, is a secure critical infrastructure. The internet is an open connection of diverse networks. Control networks need different security than general business communications. This includes using network embedded security controls to help reduce risks and to simplify security infrastructure.

10. **Privacy laws**: This final challenge is currently being legislated worldwide. We need to balance privacy with the need to gather information that can help address security breaches or fraud, while complying with associated legislation.

3. Traditional network management systems

Traditionally, datacenter network infrastructure for large organization was built based on a three-layer hierarchical model, which Cisco calls the hierarchical inter-

networking model. It consists of core layer switches ($$$) which connect to distribution layer switches ($$) (sometimes called aggregation switches), which in turn connect to access layer switches ($). Access layer switches are frequently located at the top of a rack, so, these are also known as top-of-rack (ToR) switches. Most network infrastructure is still laid out this way today.



The Hierarchical Model in a Datacenter Network Switching Architecture

The problems with this typical hierarchical networking multiply when virtual machines run on the servers, when the servers in the racks are running virtual machine managers and virtual machines, limits abound. East-west traffic is even more prevalent, because virtualization essentially randomizes the locations of the (virtual) servers.

With traditional architecture, the iNOC manager could load a rack with components that were likely to communicate with each other (say application servers and database servers). With virtualization those components could be anywhere within the virtualized infrastructure.

Virtualization also pushes the limits of IP addressing. For example, the maximum number of VLANs is 4096 (a limit based on the IEEE 802.1Q standard), which can drive artificial limits within a virtualized facility. While a facility might naturally need thousands of VLANs for multi-tenancy, because of the VLAN limit the facility may need to be divided into multiple small virtualization clusters. This limits resource management options, for example preventing a VM from being able to be moved to the least loaded server if that server is in some other cluster.

Other bad news is delivered if the iNOC managers want to make any changes to

their existing architecture. Once this hierarchical infrastructure is put in place, change is difficult. Another rack of gear not only means another ToR switch, but possibly another aggregation switch or even more ports in the core switch. If an application running in a rack needs more throughput, how is it delivered? Trunking multiple ethernet connections into a single host helps, but what if the throughput is needed to applications running in other racks? With Spanning Tree Protocol (STP), there are serious limits to how many connections can be added between the switches, leading to bottlenecks above and beyond the existing high latency.

A more modern design flattens this hierarchical network to increase performance for east-west traffic. Those networks remove the aggregation layer, requiring more ports in the core layer (with variations depending on the networking vendor). While that does provide step-wise improvement over the previous designs, it still suffers in the areas of flexibility, performance, manageability, functionality and cost.

4. Discussion

iNOCs analyze problems, perform troubleshooting, communicate with site technicians and other iNOCs, and track problems through resolution. When necessary, iNOCs escalate problems to the appropriate stakeholders. For severe conditions that are impossible to anticipate, such as a power failure or a cut optical fiber cable, iNOCs have procedures in place to immediately contact technicians to remedy the problem.

Primary responsibilities of iNOC personnel may include:

- Network monitoring
- Incident response
- Communications management
- Reporting problems

iNOCs often escalate issues in a hierarchic manner, so if an issue is not resolved in a specific time frame, the next level is informed to speed up problem remediation. iNOCs sometimes have multiple tiers of personnel, which define how experienced and/or skilled a iNOC technician is. A newly hired iNOC technician might be considered a “tier 1”, whereas a technician that has several years of experience may be considered “tier 3” or “tier 4”. As such, some problems are escalated within aiNOC before a site technician or other network engineer is contacted.

iNOC personnel may perform extra duties; a network with equipment in public areas (such as a mobile network Base Transceiver Station) may be required to have a

telephone number attached to the equipment for emergencies; as the iNOC may be the only continuously staffed part of the business, these calls will often be answered there.

4.1 Advantages

Integrated Network operation centre provides following advantages:

- Online Unified View of the entire network resources via the horizontal integration of high-level management information from Element Management Systems.
- Generation of useful synoptics for the network operator, with the ability to export views to actual end users.
- Offline Network History Summary, which complements the online view with long-term availability and performance information, allowing for the independent verification of Service Level Agreements (SLAs) with telecommunications operators.
- Service Management Views, which present the end-to-end application view as perceived by the end user, thereby aggregating the management information of the various elements that provide the service.
- Automated Connection Management, which ensures reliable and efficient activation and release of on-demand communication resources according to high-level communication service schedules coming from mission operations.

This is also useful for automatic initiation of preplanned recovery procedures if, for instance, performance degradations or failures are detected.

5. Conclusion

With increased use of internet it becomes mandatory for the Government to use system like iNOC for network management for the sake of security.

Data security and protection of confidential information being the topmost priority of the Government.

Much wider scope of the implementation of such systems to provide fast and secure access , also to control congestion as well.Future of this system seems bright as governmental organizations are implementing it for security purposes.

6. References

Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson,L., Fels, S. and Fisher, B. (2007)Towards Understanding IT Security Professionals and Their Tools. *Proceedings of ACM SOUPS*, 100-111.

Brown, J.M., Greenspan, S. and Biddle, R. Complex activities in an Operations Center: A Case Study and Model for Engineering Interaction. Proceedings of ACM EICS

"History of Network Management". Retrieved 25 August 2012.

Jeff Cormier (2011). "Exclusive : Inside AT&T's top-secret Network Operations Center (NOC)". Retrieved 25 August 2012.

"Network Operations Center opens to handle satellite bandwidth". *25 July 2012*. Retrieved 25 August 2012.

Todd Haselton (2011). "A Look Inside AT&T's Global Network Operations Center (GNOC)". Retrieved 25 August 2012.