IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Network Security Management and Protection using UTM Firewall

Pratap Singh Solanki[1*], P. R. Khatarkar[2]

[1,2]Central Water and Power Research Station, Pune, India

*Corresponding Author: solanki_ps@cwprs.gov.in, Tel.: +91-9420423171

DOI: https://doi.org/10.26438/ijcse/v7i6.10551058 | Available online at: www.ijcseonline.org

Accepted: 12/Jun/2019, Published: 30/Jun/2019

Abstract— Information and Commutation Technology (ICT) is the most important strategic issue for any organization and in the age of digital industrialization, every establishment uses the ICT for running their business therefore they are more depended on network. Increasingly uses of ICT posing new security challenges. Network infrastructure is essential to enable the network for communication. All devices in network are equally important to run the network and in failure of any one device may have devastating effect on people, economy, government services and national security. In this hyper-connected world, protecting our network and data from unauthorized access are big challenge. Process of protecting network infrastructures and data from external destructive threats and intrusion is known as network security. Network security for every organization must be consider as essential for functioning of network system and must be dealt with proactive and timely manner. For the above said purposes it is essential to have a dedicated network security system which can perform security function viz. firewall, intrusion detection and prevention, antivirus etc. In this paper we are discussing about the implementation of Unified Threat Management (UTM) Firewall system for network security management and protecting the Network for CWPRS Local Area Network (CLAN). The UTM Firewall has been successfully implemented at CWPRS for indentifying and protecting the Network from internal and external threats.

Keywords—Network security, Network threats, UTM Firewall, ICT, Internet.

I. Introduction

In this digital era, uses of Internet are growing rapidly and with this many network related threats also increased therefore it has become very challenging task to protect the Network. Network infrastructure viz. computer hardware, software, operating system, database, cable, communication media, network switches, computer application, Internet etc. are essential to enable the network for communication. All devices in network are equally important to run the network and in failure of any one device may have devastating effect on people, economy, government services and national security. Firewall protects the network from un-trusted network by filtering the contents as per organizations defined policy. Unified Threat Management (UTM) system is a network security system which provides multiple security function to protect the network from external destructive threats. Intrusion detection/prevention, gateway antivirus and anti-spam, content filtering, reporting etc. are the main features of the UTM Firewall.

Information and Communication Technology: The present age is ICT age and it is pervasive and ubiquitous. ICT is touching the life of everyone in many ways and now we are more depend on it. Today, the communication systems have become an integral part of everyday life and we are increasingly interested to connect our self in global web world. ICT has become the backbone for government organization, research and academic institutes, corporate, e-commerce, health sector, banking, finance, navigation etc. Internet is the greatest, revolutionary and advanced technology to share and published the information but at the same time it is very necessary to protect the information from destructive interaction.

Firewall: A firewall is a way to restrict access between the Internet and your internal network. You typically install a firewall at the point of maximum leverage, the point where your network connects to the Internet. The existence of a firewall at your site can greatly reduce the odds that outside attackers will penetrate your internal systems and networks. The firewall can also keep your own users from compromising your systems by sending dangerous information unencrypted passwords and sensitive data to the outside world [1]. Firewall may be roughly classified as personal and network based. Personal Firewall is software firewall and run with operating system and also known as Host-based Firewall. Mostly, Personal Firewall comes with operating system as built-in application to protect the individual Host. Network based Firewall consist Hardware, Software and Firmware. These all provides a higher performance compare to Personal Firewall. Network Firewall advantages are Simplifying security management, Advance logging and Monitoring, Creation of VPN using IPSec, hiding IP Addresses of Client Station in an internal Network by presenting one IP address to outside world etc. [2]. This paper are based on the implementation of UTM Firewall Network Security System at Central Water and Power Research Station (CWPRS), Khadakwasla, Pune, India

Unified Threat Management (UTM): As the network based devices are increasing day by day and with this, data security threats are also growing rapidly. The attacker shown their expertise to find and exploit the security holes to target the sensitive institutes, defense establishment, financial departments etc. Organization uses various types of security devices to protect the network. For Managing and monitoring, these devices take lot of efforts and expertise which puts undue pressure on the network administrators to keep updated all devices. To overcome on all such type of problems a dedicated security system required which can perform many security functions all together. Unified Threat Management (UTM) product is a powerful security system with optimized hardware and software. UTM can perform much function together viz. Firewall, intrusion detection and prevention, VPN, Antivirus etc. It is layered integrated protection system with a single appliance with minimum administrative intervene. UTM firewall are easy to deploy and reliable therefore becoming more attractive for providing comprehensive security solution. Some UTM Firewall Viz. Check Point, Cyberoam, Watch Guard, Fortigate, Sophos, Juniper SSG, Sonicwall etc.

IT Security Threats: As per Cisco blogs.cisco.com [3] some of the most common security threats are:

(1) Malware
(2) Computer Virus
(3) Rogue Security Software
(4) Trojan horse
(5) Malicious Spyware
(6) Computer Worm
(7) Botnet
(8) Spam
(9) Phishing

II. Related Work

CASE STUDY BACKGROUND AND EXISTING SYSTEM: These discussions are based on the implementation of UTM Firewall Network Security System at Central Water and Power Research Station (CWPRS), Khadakwasla, Pune, India. CWPRS is having campus-wide Local Area Network (LAN) which is extensively used for accessing e-mail, Internet, e-governance activities, Bio-metric System, Research related activities, Government e-Market (GeM), Public Finance Management System (PFMS), e-Payment etc. The installation of the LAN was carried-out by C-DAC, Pune. The existing system was equipped with multiple level network security system. Firewall with features MAC/IP binding and IPS/IDS enabled, Proxy and cashing appliance for proxy solution and appliance based antivirus solution to protect the network from virus threats. These all were appliance based solution. [4] CWPRS is a research organization and became the central agency to cater the R&D needs of the projects in the field of water and energy resources development and water-borne transport. CWPRS provides specialized services through physical and mathematical model studies in river training and flood control hydraulic structures, harbors, coastal protection, foundation engineering, ship hydrodynamic etc. CWPRS also uses various Network based software Viz. Hydrological and Mathematical Modelling, Remote sensing, AutoCAD software etc. Using CWPRS LAN to execute/study the R&D activities. CWPRS has also received instruction/guideline from Ministry of Water Resource and River Development (MoWR,RD) to implement the Crises Management Plan (CMP) for countering Cyber Attacks & Cyber Terrorism and nominate the nodal officer for Chief Information Security Officer (CISO). Therefore it was essential to have a centralized gateway level security system and web filtering mechanism to protect the CWPRS LAN system from external threats. The objective was to have single gateway level network security system with web based interface, ease of use/control and cost effective network solution to protect the CWPRS LAN from external destructive threats.

Objective: As per [5] CERT-in, the main objective of security are, Information is available and usable when required and the system that provide it can appropriately resist attacks and recover from failure (availability). Information is observed by or disclosed to only those who have a right to know (confidentiality). Information is protected against unauthorized modification (Integrality), Business transaction as well as information exchanges between organization locations or with partners/users can be trusted (authenticity and non-repudiation). Keeping in the view the above said CERT-in objective, the following were the targets to achieve using centralized UTM Firewall

- Should have the Centralized Network Security system.
- Should have easy to use and user friendly web based management tools/console.
- To Implement the LAN security policy for protecting the LAN from external and internal threats.
- To control the traffic flowing to and from the internal network to the Internet.
- Should have facility for Web/Applications filtering and blocking using customized category/policy.

- Management and supervision of user accounting and user log information.
- Gateway level antivirus/anti spam solution.
- Providing caching and proxy solution.
- Network monitoring facility.
- Qualities of Service (QoS) function for better service.
- Logs and Report generation.

III. METHODOLOGY

CWPRS is having campus-wide local area network (TCP/IP based protocol) which spread over an area of 180 hectares and encompasses more than four hundred network devices Viz. Desktop Computer, Servers, Workstation , Network Switches, Network Printer, Bio-metric attendance devices , Wi-Fi routers etc. Optical Fiber Cable (OFC) lay down for providing the network connectivity to the network switches. CWPRS is having 50 Mbps Internet Lease Line through BSNL. The LAN facility available at various Offices/Divisions share and exchange information over the network through different Servers/Workstation installed in the Data Center. The Network infrastructure is being extensively used for MIS, Internet/Intranet, Emails, Database Management, AEBAS (Bio-metric), e-Governance activities, PFMS, e-HRMS, GeM, Centralized Antivirus Security System, Remote Sensing & Mathematical Modeling, Data Acquisition, Presentation, Library management etc. To protect the IT infrastructures, software, and data from unauthorized access, it was essential to upgrade the network security system. CWPRS upgraded the existing security system with UTM firewall which equipped with many features/functions.

IV. RESULTS AND DISCUSSION

IMPROVEMENT OF ORGANIZATIONAL AND NETWORK EFFICIENCY USING UTM FIREWALL: CWPRS Network is now having the centralized UTM Firewall system to protect the Network. This UTM firewall is facilitated with many web tools. Earlier system were having multiple devices to protect the network and it was also a difficult task to manage those all devices. This Centralized Network Security system has user friendly web based management tools/console to see/check the traffic flowing to and from the internal network to the Internet. Web/Applications filtering and blocking using customized category/policy helped a lot to easily block the unwanted websites. It is having easy to use and user friendly user accounting, management, and user log information. Gateway level antivirus/anti spam security feature helps to scan suspicious contents on gateway level. Caching and proxy solution is also available in UTM. Qualities of Service (QoS) function are also helps a lot for better service. Now we can take the backup of the system and any moment and restore easily in case of failure/re-installation. User Logs and various types of Report help a lot to management for supervising and taking the decision. User can also log-in using their account name and password to check own log/access information.

RESULTS: With the aim of above said objective, CWPRS installed UTM Firewall in CWPRS LAN. This UTM system is having web-based interactive user friendly interface to view/control/manage the network using a web application. Web tools viz. centralized user accounting, live connection, quality of service, gateway level security, web filtering, traffic discovery, logs, facility to configure two ISP etc. are helping a lot to the network administrator for smooth functioning and protecting the network from external threats. After implementing this, now we are able to customize the Policy for protection of critical information and infrastructure using UTM Firewall.

V. CONCLUSION AND FUTURE SCOPE

The discussed UTM Firewall is capable to handle the present threats/challenges as per CWPRS needs. The hardware details of all network devices viz. Desktop Computer, Network Switches, Printer, Wi-Fi Router etc. Would be helpful to manage and control the hardware inventory.

ACKNOWLEDGMENT

I am very grateful to Dr. Mrs. V.V. Bhosekar, Director, CWPRS, Pune, for institutional support & continuous encouragement for according permission to publish the research paper. The implementation of Network Security System owes its credential due to the constant inspiration rendered by CWPRS officers and Nodal Officer CISO CWPRS, without whom this new technology would have not implemented. I am also thankful to Shri S.D.Ranade, Scientist-E & Nodal Officer e-Governance for timely suggestions and encouragement in every step.

REFERENCES

[1] Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman, *"Building Internet Firewalls",* Second Edition, June 2000, ISBN: 1-56592-871-7, page no. 1.

[2] Thaier Hayajneh, Bassam J. Mohd , Awni Itradat, and Ahmad Nahar Quttoum *"Performance and Information Security Evaluation with Firewalls"*, International Journal of Security and Its Applications,Vol.7, No.6 (2013), pp.355-372.

[3] https://blogs.cisco.com/smallbusiness/the-10-most-common-security-threats-explained

[4] http:cwprs.gov.in website

[5] Cert-In, Information Security Policy for protection of critical information and infrastructure CERT-in/NISAP/01, issue 01, May 2006

Authors Profile

Mr. Pratap Singh Solanki did his Bachelor of Science & Master of Computer Application degree from DAVV University Indore (M.P.). Presently he is working as Scientist-B in Central Water & Power Research Station (Govt. of India,MoWR,RD&GR), Khadakwasla R.S. Pune since October 2002 and having more than 15 years of industrial and research experience in the field of Software Development, Database Management, Computer Network, Cyber Security, e-Governance activities , System Administration, Web Development, Government e-Marketing (GeM) etc. He has successfully in-house developed and implemented various Clients /Server & Web based Applications. His area of interest of research is Database Management, Data Mining , Cyber Security and Integrated Water Resource Management.

Mr. P.R.Khatarkar is having Bachelor of Engineering (E&TC) and Master of Technology (IT) degree and presently he is working as Scientist-D in Central Water & Power Research Station (Govt.of India, MoWR,RD&GR), Khadakwasla R.S. Pune since December 1989 and having more than 30 years of industrial and research experience in the field of Computer Network, e-Governance activities , System Administration, National Hydrology Project etc. He has also implemented various e-governance projects/activities at CWPRS as per Govt. Guidelines. He is also working as Nodal officer for Chief Information & Security Officer (CISO) for CWPRS LAN which comprises more than 450 network (wired and wireless) devices. His area of interest of research is Network Security.