# A Network Infrastructure for Security Enhancement

Shikha Verma

ABES Engineering College Ghaziabad, India

Corresponding author: Shikha Verma, Email: shikhasaxena83@gmail.com

Security is big concern for an organization. All the work done in any organization should be secure and protected from unauthorized access.The physical arrangement of workstation forms topology. Organization's most commonly used topologies are star and ring. Paper also presents architecture for an organization that is most protected from failure. To ensure security, organization should use port level security.Securedports help to limits the workstation to be connected to the port. This helps in security as well as traffic management. The paper also presents the maintenance of syslog server to check unauthorized access so that network can be protect from outside world. As the organization's LAN connected to outside world so the security of routers, firewall and wireless access point is also needed.

**Keywords**: Firewall, Fail safe architecture, VPN, WAN, LAN, VLAN, CISCO, Log Parser,SNMP,WAP, Port security.

2023. In Saroj Hiranwal & Garima Mathur (eds.), *Artificial Intelligence and Communication Technologies*, 147–151. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-955020-5-9-14

# 1 Introduction

Security of network is necessary in present era. As many people send their private data on public network. To define network architecture, the security, logging, and forensic data–gathering methodologies must be considered. The following sections of this paper describe about how to design a secure network, how to define port security andalso discuss a provision provided by Microsoft tool log parser and inclusion of the devices like firewall router and switches for securing network.

# 2 Create a Secure Network Architecture

To create a failsafe structure, first create a topology that is combination of star topology and ring topology [1].In order to secure fail safe architecture firewall can be used. Firewall work as a safe guard for LAN. To access resources of firewall VPN connection is required. On the VPN, syslog server, Log Parser, PING sweep, failsafe topology log entries are made by VPN connection that shows successful attempts as well as fail attempts. Transmission of data from firewall to workstation should be in encrypted formand that is ensure by virtual private network (VPN) connection. There is need for creating failsafe architecture with security as in fig 1. Default settings of the switches give the chances to the attackers to attack in the network. So Cisco switch can be used.That is able to provide security at port level and diversity of different levels.

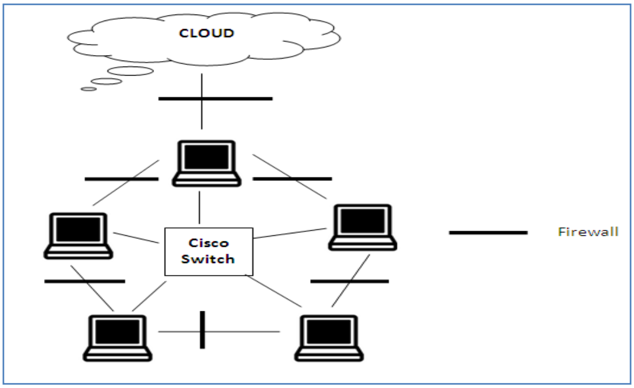

**Figure1:** Fail safe structure with firewall

# 3 Port Security to Secure Network

To restrict the input on interface port security is popularly used. On a port there is restriction to use workstations to gain security [9]. A secure MAC address is assigned to secure ports. Ports that don’t have secure MAC addressesare not able to forward packets. A port can also be configure as secure port, now if the workstation (don’t have secure MAC) attempts to access that port then security violation occurs.

Maximum number of secure MAC addresses can be set on a port. The secure addresses are included in an address table by port-security, MAC_address interface configuration command. This may also be done by allowing the port to dynamically configure secure MAC address with the MAC address of connecting devices. A security violation occurs if a workstation whose MAC address is not in the address table and it try to access the interface. For this volition mode interface can be configured on following violation modes

**a) Restrict**—A port security violation restricts data. The default counter value is set to 1.The counter of Security Violation increments that generates SNMP Notification.

**b) Shutdown**—A port security violation causes the interface to shut down immediately.

### 3.1 Configuring Port Security and Aging

Port Security as well as aging can be configuring on any particular interface to achieve security. With the help of these configurations traffic on network can also be controlled. Port security aging is use to set the aging time and aging type is used for port security for all secure addresses. Aging helps for limiting the number of secure addresses on a port and without manually deletion, port can be disable. 0 to 1440 minutes is valid range for aging time. Aging is disabled for this port if time is 0. Examples defined below can be used to achieve port security and aging:

- To enable port security on Fast Ethernet port 11
  ```
  Switch(config)# interface fastethernet 3/11
  ```
- To set violation mode is the default
  ```
  Switch(config-if)# switchport mode access
  ```
- To set the maximum number of secure addresses to 11
  ```
  Switch(config-if)# switchport port-security
  Switch(config-if)# switchport port-security maximum 11
  ```
- To secure MAC addresses configured.
  ```
  Switch(config-if)# switchport port-security mac-address 70:71:BC:49:93:6E
  Switch(config-if)#  switchport port-security mac-address sticky 70:71:BC:49:93:12
  ```
- To set the aging time 3 hours
  ```
  Switch(config)# interface fastethernet 3/11
  Switch(config-if)# switchport port-security aging time 180
  ```
- To set the aging time  2 minutes:
  ```
  Switch(config-if)# switchport port-security aging time 2
  ```
- To show port-security for interface for verifying entries
  ```
  Switch# show port-security interface fastethernet 3/11
  ```

Similarly rate limit for bad packets, privileged EXEC mode and MAC address table can be defined.

## 4 Gaining Security by Use of Log Parser

There is need to maintain syslog server to notice the activities happens on the router and switches so that network can be prevented from outside attackers. Microsoft provide best tool that is Log Parser. Log parser use queries more similar to SQL like to fetch information from log files. Organization can maintain reports of these logs and can share with other database so that future reporting can be easily done.  Regular checking for events of log files help our organization to discover incidents.

### 4.1 Syslog

It is very much useful for organization get the knowledge of any incident in advance by monitoring the log files from network devices(devices includes routers, switches, wireless devices, and firewalls as well as servers). Log parser reads the logs and generates the repots in desirable form on daily basis or weekly basis. To build a security logging database for monthly, quarterly, biannual, and annual security reports log parser uses queries to extract the messages from logs in to reports. Logs from the routers, switches etc the organization needs to analyze. If any odd entries in these logs are found than the organization needs to get attentive and report to security department timely. Some examples of log parser queries are as follows:

- To See all the details of log file
  log parser "select * from logfile"
- To see all pages hit by particular IP in ascendingorder[11]
  log parser "select cs-uri-stem,count(cs-uri-stem) from logfile where c-ip = "172.168.3.27" groupby cs-uri-stem orderby count(cs-uri-stem) ASC"
- To see Hits on a particular page by IP address in ascending order
  log parser "select c-ip, count(c-ip) as request count from logfile where cs-uri-stem like '%authorizeduser.xls%'groupby c-iporderby count(c-ip) ASC"
- These turns to find the domain related with a given IP address
  log parser "select c-ip, REVERSEDNS(c-ip) from logfile where c-ip = '172.168.3.25' "
- To see all the hits write on CVS file
  log parser "select * into log_output.csv from logfile".

Similarly queries to see output of log files on chart and per hors hits by particular IP and so on to secure network.

# 5 Security Achieved by Routers and Switches

To create a network architecture routers play an important role. The router that is used may be perimeter router that connects our organization to the internet. This router is in contact of lot many people so is more vulnerable to attacks. Telnet connection to the outside interface, Denial of service attack, Simple Network Management Protocol (SNMP) attack are three most common types of attack on the perimeter are enabled by default. Other built in routers the organization are inter VLAN router and core WAN router. Inter VLAN uses to separate broadcast domain and move directed IP traffic. Organization and remote offices are connected by dedicated point to point connection by using WAN router.

Switches used to connect the nodes in star fashion in fail-safe secure architecture as in fig1. To get more security it is very important for an organization to use Cisco switches like CAT OS-based (5500 and 6500 series) that is core switches and is the backbone of the LAN. Different categories of network interfaces also support by this. To split a LAN in to subnetworks for higher security they use firewall cards.

Other switches like IOS based series that is 2900 and 3500 series and Menu based series or 1900 series can also be used.

# 6 Secure WAP (Wireless Access Points)

Wireless access is wide areas of network growth. When anyone in the organization works on the laptop and wants to add more wireless capability to perform their work. That time wireless security may be violate by hackers. Two commonly used wireless standards are WEP and WPA. To ensure high security from the wireless users the best way is to put a firewall between wired network and WAP. Employees of organization should use VPN for security.

## 7 Conclusion and Future Work

Security of LAN network is important to for any organization. Awareness of Log files, routers, Firewall and switches is important for an organization to ensure high security of network. The paper presented the method to secure the port by using commands and also defines ways access the Log files using logPraser. The importance of the firewall to achieve security of LAN is also discussed. There should be proper policies that tell about how to use network. Programs may be written to automate the Log Parser for log reviewing.

## References

[1] Saxena Shikha, Chandra Somnath, "Implementation and simulation of failsafe network architecture", IRJET, Volume6 Issue 5, 2019

[2] https://mlichtenberg.wordpress.com/2011/02/03/log-parser-rocks-more-than-50-examples/

[3]https://blogs.technet.microsoft.com/karywa/2013/06/05/log-parser-studio-write-your-first-query-in-less-than-30-seconds-part-i/

[4] https://conetrix.com/blog/microsoft-log-parser-beginners-guide

[5] https://www.sciencedirect.com/topics/computer-science/star-topology

[6] P. He, J. Zhu, S. He, J. Li and M. R. Lyu, "An Evaluation Study on Log Parsing and Its Use in Log Mining," 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Toulouse,pp. 654-661, 2016.

[7] HudanStudiawan, Ferdous Sohel, Christian Payne ,"Automatic log parser to support forensic analysis "Australian Digital Forensics Conference 2018

[8] Pinjia He, Jieming Zhu, Shilin He, Jian Li, Michael R. Lyu, "Towards Automated Log Parsing for Large-Scale Log Data Analysis", Dependable and Secure Computing IEEE Transactions on, vol. 15, no. 6, pp. 931-944, 2018.

[9]https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/122/25ew/configuration/guide/conf/port_sec.html

[10] RFC 3986," http://www.rfc-editor.org/rfc/rfc3986.txt"