Proc. of Int. Conf. on Current Trends in Eng., Science and Technology, ICCTEST

Network Security: Threats and Solutions

Venkatesh P [1] and TasmiyaTaranum M S [2]
[1]Don Bosco Institute Of Technology, Bangalore, India
Manjulausha127@gmail.com

***Abstract*—Network security has more become more important to personal computer users, organisations, and the military. 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. The network can be secured by the means of firewalls and encryption methods.**

***Index Terms*— Network security, Developing network security, threats and solutions, advantages and disadvantages.**

I. INTRODUCTION

Network security is a protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system.
Example: antivirus system

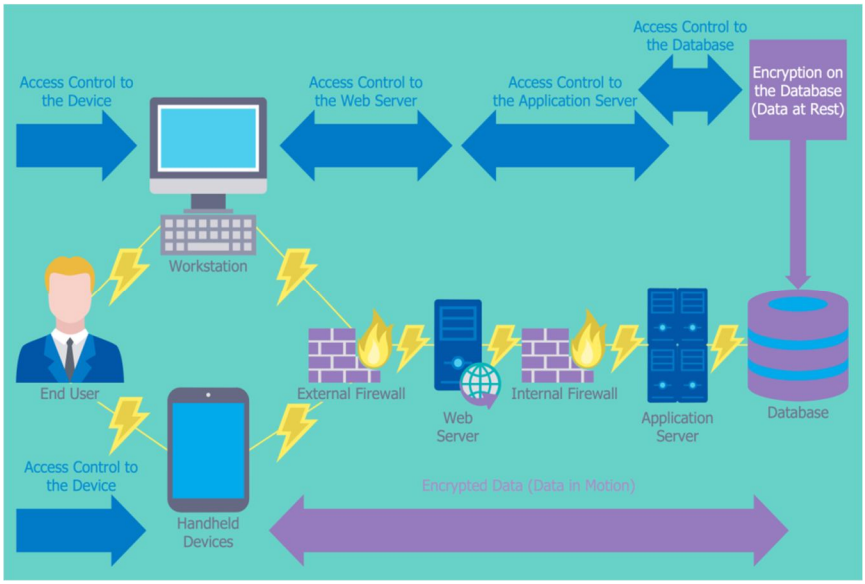


Fig 1. Network Security Diagram

Grenze ID: 02.ICCTEST.2017.1.112

II. Developing Network Security

To develop a network security the following need to be considered**:**

- Access: Authorised users are provided the means to communicate to and from a particular network.
- Confidentiality: Information in the network remains private.
- Authentication: Ensure the users of the network are who they say they are.
- Integrity: Ensure the message has not been modified in transit.
- Non-Repudiation: Ensure the user does not refute he used the network.
- Access control: Limits ant control access to certain system applications to certain users.
- Availability: ensures the service is only available to legitimated users and not available to users who do not have access to the applications.

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and the factors that make a network vulnerable to attack.

III. Network Security Threats And Solutions

A. Types of attacks

1. Passive attack: In this attack an adversary deploys a sniffer tool and waits for sensitive information to be captured. (fig.1)
2. Active attack: In this attack an adversary does not wait for any sensitive or authentication information. He actively tries to break or bypass the secured systems. (fig.2)
3. Insider attack: In this attack an attacker intentionally damage network infrastructure or data. This attack also happens due to carelessness or lack of knowledge. (fig.3)
4. Hijack attack: This attack usually takes place between running sessions. Hacker joins a running session and silently disconnects other party. Then communicate with the other active parties by using the identity of disconnected party.(fig.4)
5. Spoof attack: In this kind of attack an adversary changes the sources address of packet so receiver assumes that packet comes from someone else. This technique is typically used to bypass the firewall rules. (fig.5)
6. Password attack: In this attack an adversary tries to login with guessed password. (fig.6)

Along with these attacks there are other attacks like packet capturing attack, man in the middle attack, ping sweep attack, denial of service attack, exploit attack and more.

B. Solutions to prevent attacks of network security

Common cisco security appliances: More than 80% of the internet backbone routers are running Cisco IOS software. Cisco IOS software is the most critical part of network infrastructure. Probably it gets the most hacking attacks in the networking world. Cisco provides several products to secure the software and other networking infrastructure.

1) CISCO ASA (adaptive security appliance): This is the coolest product from Cisco. Along with working as firewall it also supports requirement specific security modules. (fig 1.1)
2) CISCO IPS (INTRUDER PREVENTION SYSTEM): This module filters all network traffic for possible attacks. If an attack signature match, it will automatically change access control lists and will create a rule to form firewall to block the attacker. (fig 2.2)
3) CISCO DDOS (DISTRIBUTED DENIAL OF SERVICE): This module filters network traffic in real time for potential DDOS attack and block malicious traffic without affecting genuine traffic. (fig 3.3)
4) CISCO ANATOMY GUARD: It maintains a normal traffic profile by analysing user behaviour. It can detect any deviation from normal traffic profile. It triggers an alert to administrator when it detects any deviation. (fig 4.4)
5) CISCO SECURITY AGENT (CSA): This module works like antivirus software. But it has more features than antivirus software. (fig 5.5)
6) NETWORK ADMISSION CONTROL: This module administrator can quarantine and prevent unauthorised access from end users. (fig 6.6)
7) SECURITY MONITORING, ANALYSIS, AND RESPONSE SYSTEM (mars): This module is used for monitoring security devices and host applications. It also responses for the threat on network.(fig 7.7)

Along with these there are many other security technologies used for prevention of attacks.

TABLE I. TABLE SHOWING VARIOUS NETWORK SECURITY TECHNOLOGIES BEING USED

Computer Security attributes	Attack Methods	Technology for Internet Security
Confidentiality	Eavesdropping, HIacking, Phishing, DoS and IP Spoofing	IDS, Firewall, Cryptographic Systems, IPSec and SSL
Integrity	Viruses, Worms, Trojans, Eavesdropping, DoS and IP Spoofing.	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Privacy	Email bombing, Spamming, Hacking, DoS and Cookies	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Availability	DoS, Email bombing, Spamming and Systems Boot Record Infectors	IDS, Anti-Malware Software and Firewall.

IV. ADVANTAGES AND DISADVANTAGES OF NETWORK SECURITY

A. Advantages

1. Protects data
2. Prevents cyber attack
3. Levels of access
4. Centrally controlled

B. Disadvantages

1. Costly setup
2. Time consuming
3. Requires skilled staff
4. Careless admin

V. CONCLUSION

Network security is an important field that is increasingly gaining the attention as the internet expands. The security technology is mostly software based, but many hardware devices are also used.
Use of security tools such as firewalls, intrusion detection, and authentication mechanism will prove effectively in guarding intellectual property for the near future. The network security field may have to evolve more rapidly to deal with the threats further in future.

REFERENCES

[1] CURTIN, M. “Introduction to network security”, http://www.interhack.net/pubs/network-security.
[2] “Improving security”, http://www.cert.org/tech_tips,2006.
[3] OHTA. T.; CHIKARAISHI. T., “Network security model”, networks, 1993. International conference on engineering ’93. ‘communications and networks for the year 2000’, proceedings of IEEE Singapore international conference on, vol.2, no., pp.507-511 vol.2, 6-11 Sep 1993.
[4] ADEYINKA, O., “Internet attack methods and internet security technology”, modelling and simulation, 2008. AICMS 08. Second Asia International conference on, vol., no., pp.77-82, 13-15 May 2008.

Fig1

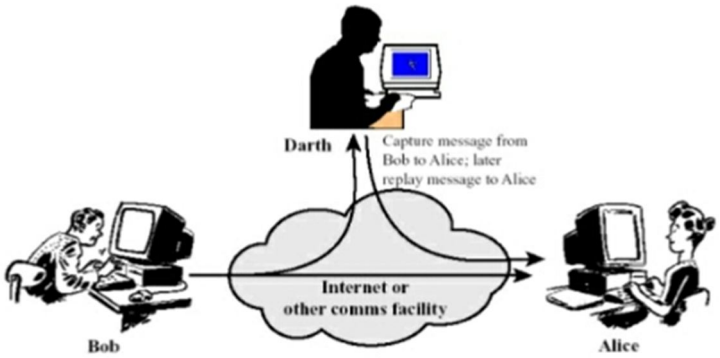


Fig 2

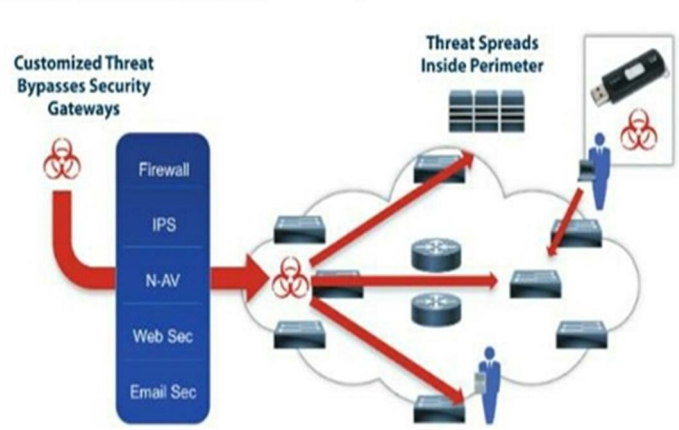


Fig 3

Fig 4

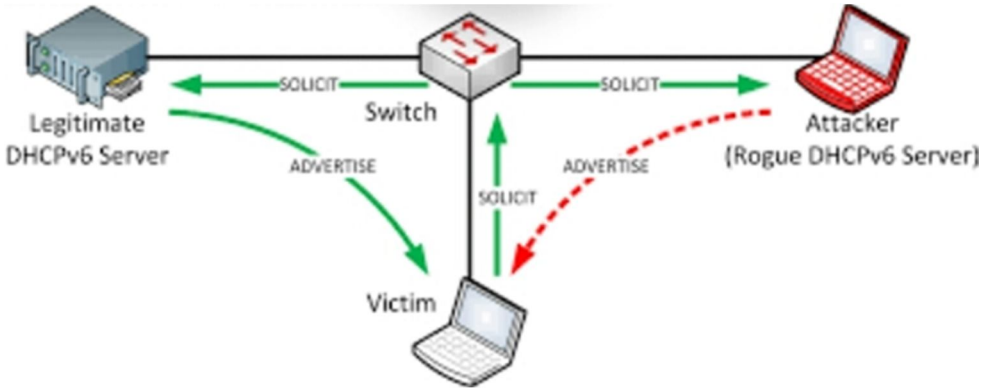


Fig 5

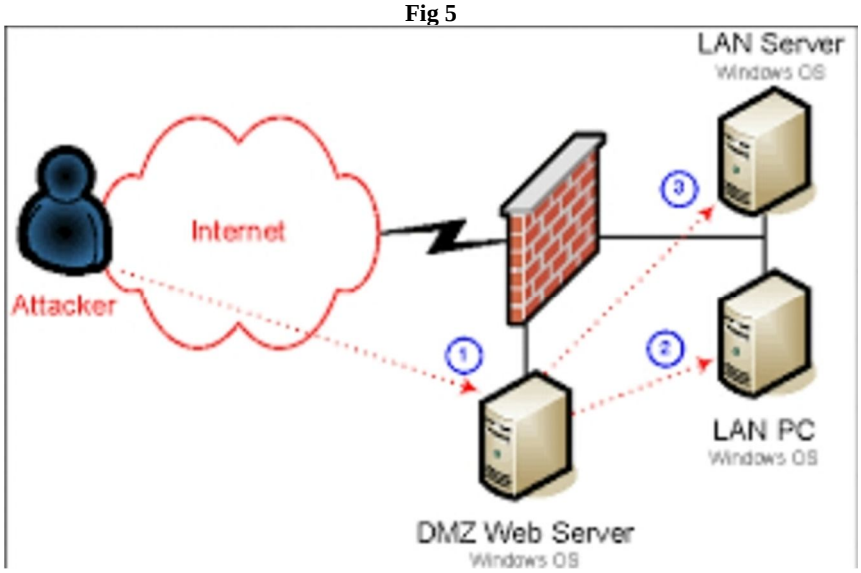


Fig 1.1

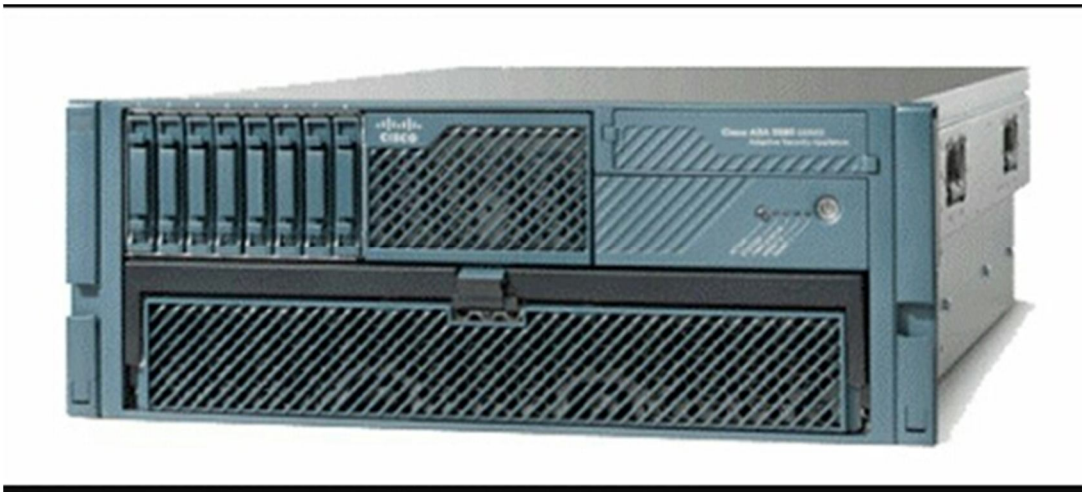


Fig 1.2

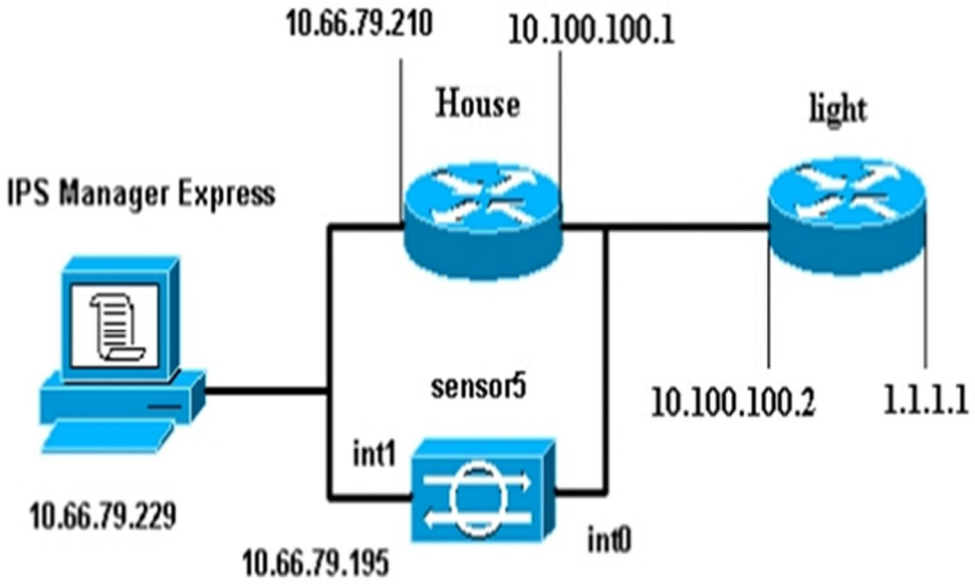

10.66.79.210
10.100.100.1
House
light
IPS Manager Express
sensor5
10.100.100.2
1.1.1.1
int1
10.66.79.229
int0
10.66.79.195

Fig 1.3

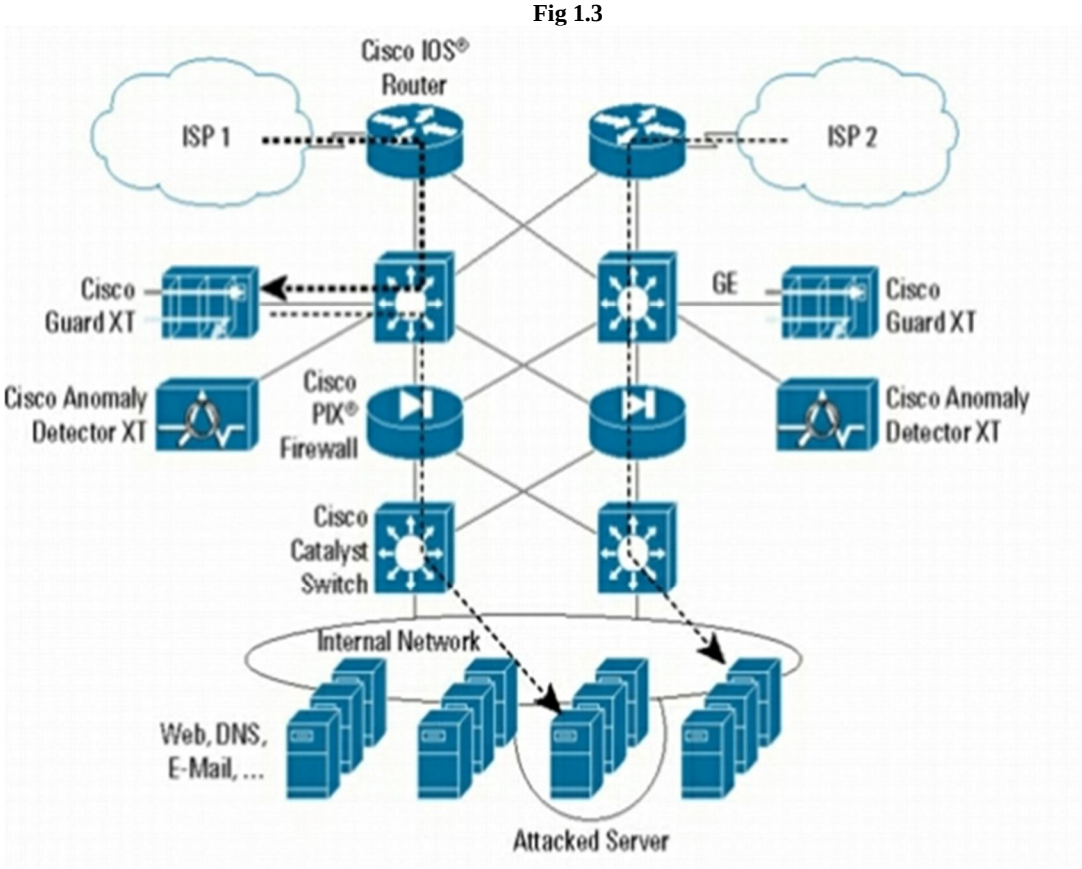

Cisco IOS®
Router
ISP 1
ISP 2
Cisco
Guard XT
GE
Cisco
Guard XT
Cisco Anomaly
Detector XT
Cisco
PIX®
Firewall
Cisco Anomaly
Detector XT
Cisco
Catalyst
Switch
Internal Network
Web, DNS,
E-Mail, ...
Attacked Server

Fig 1.4

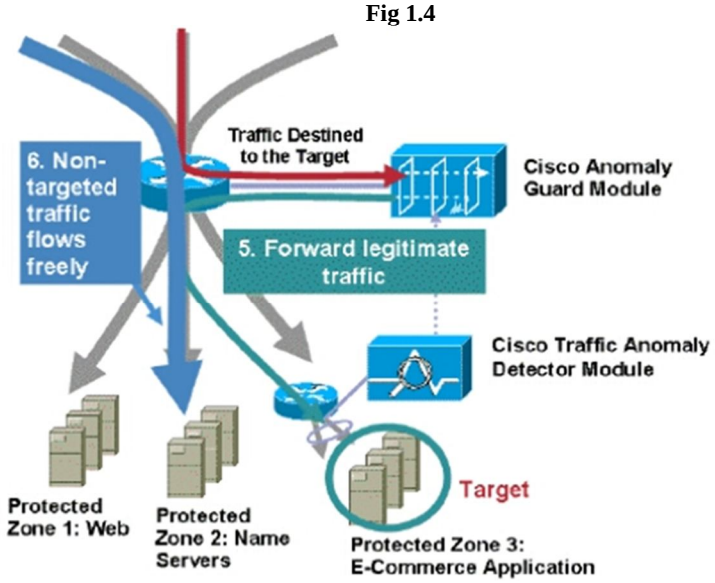


Fig 1.5

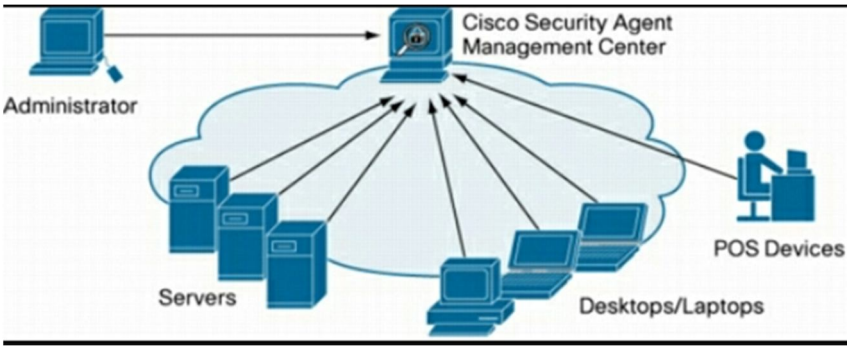


Fig 1.6

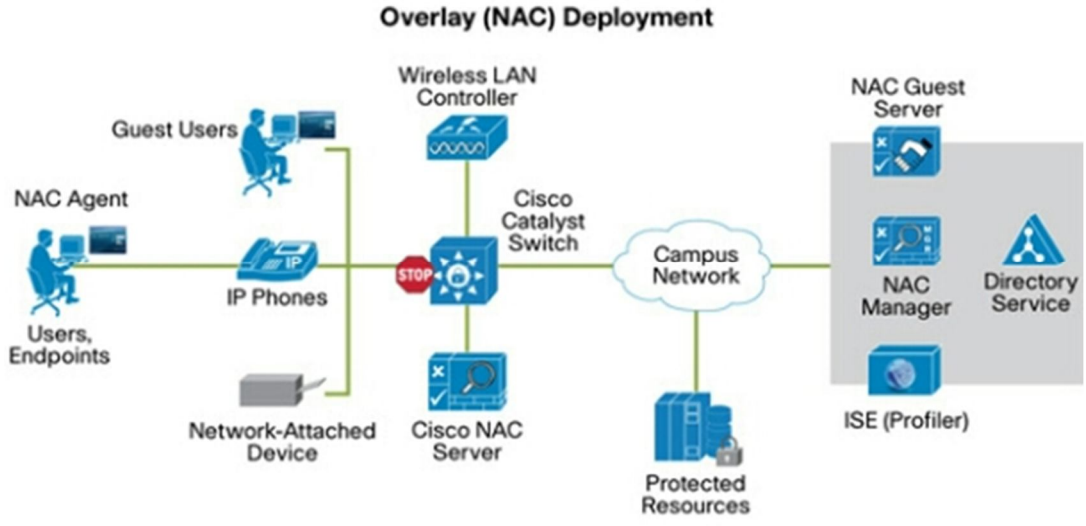
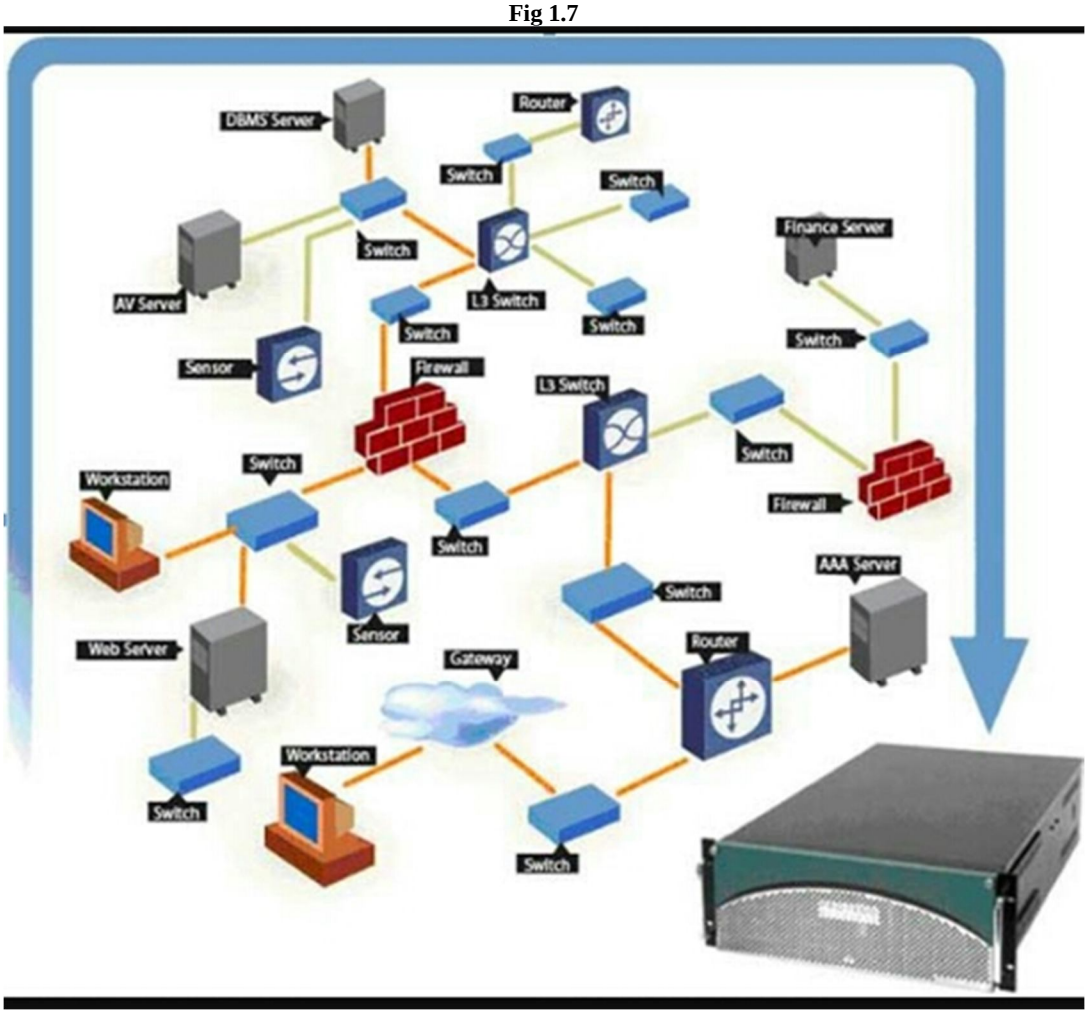


Fig 1.7


DBMS Server
Router
Switch
Switch
Switch
AV Server
L3 Switch
Finance Server
Switch
Switch
Switch
Sensor
Firewall
L3 Switch
Switch
Switch
Workstation
Switch
Firewall
Switch
AAA Server
Switch
Sensor
Web Server
Gateway
Router
Workstation
Switch
Switch