Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Engineering

Diploma Thesis

Computer networks in SMEs

Ahmed Munir

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Ahmed Munir

Systems Engineering and Informatics
Informatics

Thesis title

Computer networks in SMEs

Objectives of thesis

Diploma thesis is focused on problem of computer networks in small and medium enterprises. The main objective is analyses of selected computer network technologies and topologies.
Partial goals of this work is characteristics of computer network technologies.

Methodology

Methodology of the diploma thesis is based on study and analysis of specialized information sources. The practical part is focused on analyse and comparison of selected computer network technologies and topologies creating of computer network in SME. Based on a synthesis of theoretical knowledge and the results of own solution, the conclusions of the thesis will be formulated.

The proposed extent of the thesis

60 – 80 pages of text.

Keywords

Computer network, LAN, WAN, Protocols, network devices

Recommended information sources

AL-BAHADILI, Hussein. Simulation in computer network design and modeling: use and analysis. Hershey, PA: Information Science Reference, c2012. ISBN 9781466601932.

BROOKS, R. R., c2014. Introduction to computer and network security: navigating shades of gray. Boca Raton: CRC Press. ISBN 978-1-4398-6071-7.

KÁLLAY, Fedor and Peter PENIAK. Computer networks and their applications: LAN / MAN / WAN . 2. upd. Praha: Grada, 2003. ISBN 80-247-0545-1.

Literature KUROSE, James F. and Keith W. ROSS. Computer networks . Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

MARCHETTE, David J., c2001. Computer intrusion detection and network monitoring: a statistical viewpoint. New York: Springer. ISBN 0-387-95281-0.

MCMILLAN, Troy. Cisco networking essentials. Second edition. Indianapolis, Indiana: Sybex, [2015]. ISBN 1119092159.

MCQUERRY, Steve. Interconnecting Cisco network devices. 3rd ed. Indianapolis, Ind.: Cisco Press, c2008. Self-study guide series. ISBN 1587054639.

ODOM, Wendell, Russian HEALY and Naren MEHTA. Network Routing and Switching: Authorized Tutorial . Brno: Computer Press, 2009. Self-study. ISBN 978-80-251-2520-5.

OSI, the open systems networking standard. Charleston, S.C.: Computer Technology Research, 1993. ISBN 1566070147.

Expected date of thesis defence

2020/21 WS – FEM (February 2021)

The Diploma Thesis Supervisor

Ing. Pavel Šimek, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 11. 10. 2019	Electronic approval: 14. 10. 2019
Ing. Jiří Vaněk, Ph.D.	**Ing. Martin Pelikán, Ph.D.**
Head of department	Dean

Prague on 26. 11. 2020

Declaration

I declare that I have worked on my diploma thesis titled " Computer networks in SMEs" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the diploma thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on ....

Munir Ahmed

Acknowledgment

I would like to thank my supervisor, Ing. Pavel Simek, Ph.D., for his guidance and helpful advice while working on the thesis. Many thanks also go to the other colleagues from the CZU. Finally, I am grateful to my family and friends for their love and support. Thank you all.

Author

Ahmed Munir

Computer networks in SMEs

Abstract

This study was performed about Small and medium-sized enterprises computer networks as SMEs are very popular. Small and medium-sized enterprises (SMEs) represent almost 99% of all European Union (EU) businesses. Computer networking and information technology play a vital role in the professional world, and it ensures maximum efficiency and productivity of any company or organization. Employees share their idea more easily and efficiently with clients. When an employer is connected with their desire clients, company income, and productivity increase significantly. Companies and clients always share their sensitive data over the computer network as the computer network is faster than other mediums. But today's world is not as secure as it can be imagined. Internet is full of security risk because a lot of cybercrime are happening every day. Not only a big company is facing internet security threats, small and medium-size enterprise-facing more security threats because the Number of SMEs is remarkably huge than a big company. So, securing a computer network is very important for the business. This paper will describe a few important things playing a vital role in computer network security.

Keywords

Computer network, LAN, WAN, Protocols, network devices, Network security.

Table of Contents

List of figures

List of tables

List of abbreviations

VLANs	Virtual Local Area Network
ACL	Access Control List
AAA	authentication, authorization, and accounting
(TACACS+)	Terminal Access Controller Access-Control System Plus
DMZ	Demilitarized Zone
IPSec	Internet Protocol Security
VPN	Virtual private networks
IOS	Internetwork Operating System
LAN	Local Area Network
CAM	Content-Addressable Memory
MAC	Media access control
STP	Spanning Tree Protocol
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
TCP	transmission control protocol
UDP	User datagram protocol
TFTP	Trivial File Transfer Protocol
IETF	Internet Engineering Task Force
NIS+	Network Information Service plus
IDS	Intrusion detection system
IPS	Intrusion Prevention Systems
ASCII	American Standard Code for Information Interchange
WAN	wide area network
DDoS	Distributed Denial of Service
SFTP	SSH File Transfer Protocol
SSL	Secure Sockets Layer

TLS	Transport Layer Security
SQL	Structured Query Language
HTTPS	Hypertext Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
OS	Operating system
URL	Uniform Resource Locator
CA	Certificate Authority (CA).
SSH	Secure Shell
PGP	Pretty Good Privacy
SHA-1	Secure Hash Algorithm
RSA	Rivest, Shamir, and Adelman
ZIP	Zone Improvement Plan
MIME	Multipurpose Internet Mail Extension
S/MIME	Secure/Multipurpose Internet Mail Extension
ESP	Encapsulation Security Payload
AH	Authentication Header
WEP	Wired Equivalent Privacy
WPA	wi-fi Protected Access
SSID	service set identifier
SNMP	Simple Network Management Protocol
NBA	Network behavior system
AWS	Amazon Web Services
Iaas	Infrastructure as a service
API	application program interface
CMS	Central Management service
SME	Small and Medium Enterprises
ISP	Internet Service Provider

1. Introduction

Computer networks are all around us, and it's essential for effective communication, research and development, modern education, sharing knowledge, entertainment, and of course, for business. Day by day, small and medium-sized organizations are developing significantly due to the fact of the enhancement of communication. In Europe, there were an estimated 25.1 million small and medium enterprises (SMEs) in 2018. business owners are communicating with their clients very efficiently. A high-speed computer network provides enormous advantages and increases productivity and easy communication as well. Maintaining a computer network is not an easy task. Computer network attack is widespread.

Hackers are hacking personal data and destroying the security of the network. There are many different types of network treats available such as DDoS attacks, computer viruses, etc. Hackers target not only big sized companies; they are frequently targeting Small and medium-sized enterprise. So, data security for SMEs becomes very challenging. For instance, if one Pc infected by malware and starts to send unwanted messages, it cannot be detected as a client PC. The entire network can be affected by this. in this situation, Network monitoring becomes a handy wall. Inside the computer network, a good network monitoring system can analyze a user's daily activity and network devices' behavior. And as a result, the attack can be visible, and based on the attack; existing network security should be improved.

Network protection combines more than one layer of defenses at the part and in the network. Only Authorized customers can get access to office network resources with their given credential, but malicious actors or hackers are blocked from carrying out exploits and threats. There are few types of network security such as firewall, email security, Antivirus, and malware software, network, access control, Application security, Behavior analytics, cloud security, data loss prevention, intrusion preventions, Mobile device security, Security information, and event management, VPN, web security, wireless security, etc.

Organizations have to get entry to more precious statistics than ever before—and defending that facts are quintessential to enterprise success. Effective community security acts as a gatekeeper to that information, stopping unauthorized access, misuse, modification, or altering a laptop community and its resources.

Network protection is any system, device, or motion designed to defend the protection and reliability of a network and its data Like a fence around non-public land or a lock on a door, community safety manages to get admission to a community by stopping a vary of threats from getting into and spreading by means of a system.. The right network safety solution helps commercial enterprise continues to be compliant with enterprise and government regulations, and it will limit the enterprise and monetary have an effect on of a breach if it does occur. Network safety ensures the protection of information and records shared across the network, which is very important for SMEs.

2. Objectives and Methodology

2.1 Objectives

This diploma thesis is focused on the problem of computer networks in small and medium enterprises. The main objective is analyses of selected computer network technologies and topologies. Partial goals of this work are the characteristics of computer network technologies.

2.2 Methodology

Small and medium-sized computer networks facing lots of security threats every day. In this study, some research has been done about the most common issues of SME's computer network and how SMEs computer network can prevent those threats.

To achieve goals, few parameters are investigated.

- In the first part of this thesis, some important theories on a computer network will be discussed, such as computer network topology, network devices, services, network protocols, switching, routing, and other vital topics.
- The practical part of this thesis has prototype network design and simulation with some desire features. Some features are configured and tested: inter VLAN routing, STP, and VTP in network switches. In firewall, High availability (HA) and VPN are configured. Basic security hardening on network devices has been configured.
- The conclusive part of this thesis will cover the observation of prototype networks, which is mentioned in the second part of my thesis. Observations are focused on network performance and security for SMEs.

It is tough to think about any business without sharing information. Company and client relations strongly depend on daily conversation. A massive amount of sensitive data sharing happened within the company and clients. A functional, fast, secure computer networks help a business grow. And company productivity depends on how fast a company can interact with their customer. And these communications should be secure as the internet is full of threats. So, securing a computer network for a small and medium-sized company is very important. SMEs can have a good relationship with their customer if SMEs have a secure network, increasing their productivity and profit. Securing a computer network is not an easy task. Malware, viruses, hackers are available on the internet.

3 Literature Review

3.2 Definition of Terms

3.2.1 Network topologies

A network topology is the hubs plan - normally switches, bridges - and associations in a system, frequently spoke to as a diagram. The system's topology and the overall areas of the source and goal of traffic streams on the system decide the ideal way for each stream and the degree to which excess choices for steering exist in case of a disappointment. The aspect of its centralized nature, the network topologies offer simplification of operation (1). It also ensures the isolation of the device inside the network. There are few types of Network topology such as Bus, Start, Mesh, Hybrid network topology. In the bus network topology, all the nodes are associated with a single cable. The main cable acts as a backbone.

Nodes will be disconnected if the backbone is broken. It can be easily connected to all nodes in bus topology as all devices can connect linearly. A topology start topology where all devices are connected individually to a central device such as a hub, switch, or bridge. Start topology is most common in the computer network, and it takes more network cable (2). Only one node will be disconnected if the cable fails as it has an individual link with a central device. The mesh topology was developed for Army application, and in this topology, all nodes help distribute data amongst each other.

Mesh net can handle a high amount of data traffic as one more device can simultaneously send and receive data. The device can be added to the mesh net; it will not disrupt data transmission between other devices. Half and half topologies organize associations that utilize different techniques for connecting associations with different devices associated with the framework, such as PCs and even printers (1). These system types have a few favorable circumstances, for example, having the option to use the most grounded parts of different systems, e.g., signal quality. They likewise have a few detriments, including the prerequisite for a top of the line gear.

Nowadays, star topology is the most used network topology in an enterprise network. Using Star topology, the network can be scaled very easily and reduce the probability of network failure.

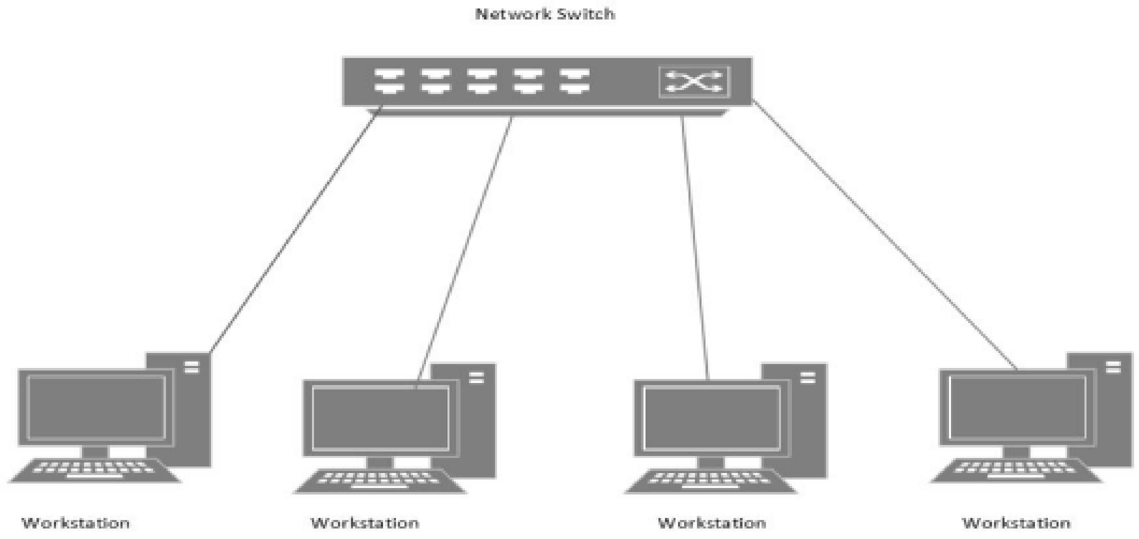


Figure 01: A star topology connecting four workstations

3.2.2 LAN and WAN

Local Area Network refers to a computer network covering a small geographical region such as inside companies, buildings, offices, and homes. In the Local Area, network computers can exchange statistics and messages smoothly and rapidly (1). Each person can proportion messages and facts with any other consumer on LAN (4). The person can log in from any laptop on the LAN and enter the same information placed on the server.

The gathering of PCs and other network devices is associated with a switch, hub, or bridge, utilizing a private tending to plot as characterized by the TCP/IP convention. In the LAN, most of the devices have private IP and those IP from DHCP server. Switches are found at the limit of a LAN, associating them to the bigger WAN. Local Area network uses Private IP address space which are from DHCP server leases. IPv4 and IPV6 both have private IP address ranges.

A wide area network is not tied to a single location, and it can play a vital role in international business and is also very useful for everyday use. It can be considered the Internet the largest WAN in the world. WAN connects multiple locations and its most expensive forms of a computer network. ISP often establishes WAN networks. ISP leases its WAN to enterprise business government, educational institute, etc. (5). Consumers can store data in different locations and communicate with others, no matter their location. WAN access can be ensured via a different link, such as a virtual private network (VPN).

All data transfer takes very little time. An employee from many locations can share their data which speed up teamwork. By WAN using, the user can stay connected for the greater data

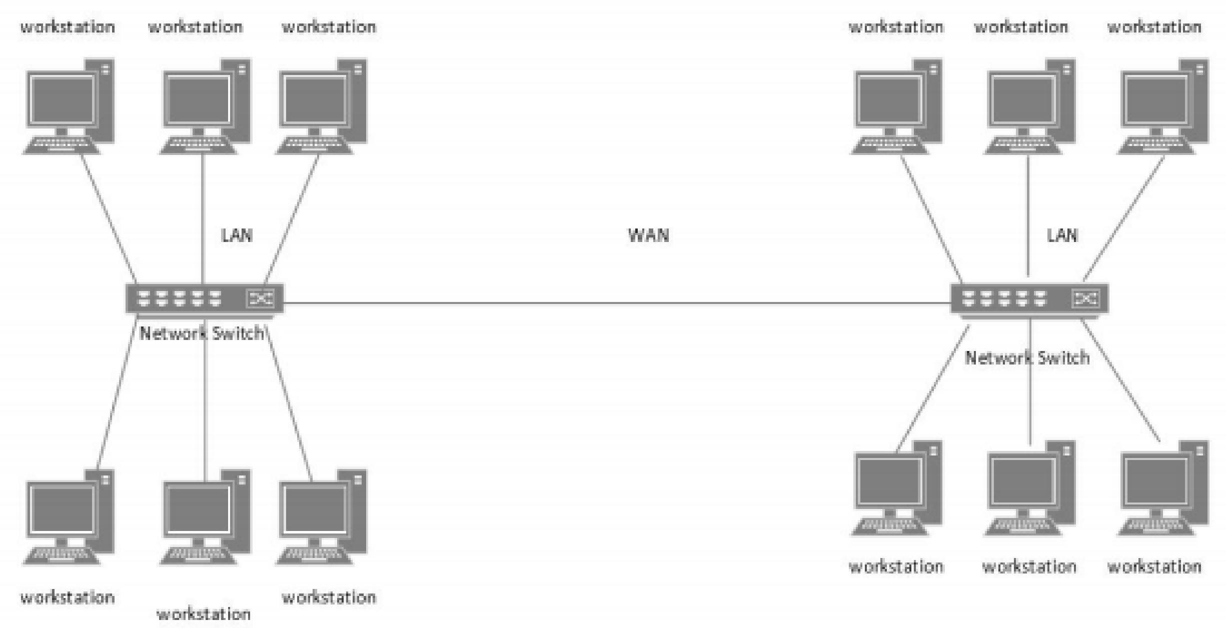


Figure 02: LAN and WAN

3.2.3 Networking protocols

System protocols are formal models, and approaches included principles, methods, and arrangements that characterize correspondence between at least two gadgets over a system. System protocols oversee start to finish auspicious, secure, and oversaw information or system correspondence (3). System protocols consolidate every one of the procedures, prerequisites, and imperatives of starting and achieving correspondence between PCs, servers, switches, and other system empowered gadgets.

System protocols must be affirmed and introduced by the sender and beneficiary to guarantee organizing/information correspondence and applying to programming and equipment hubs that convey a system. There are a few expansive kinds of systems administration protocols, including:

- **System correspondence protocols:** Basic information correspondence protocols, for example, TCP/IP and HTTP.

- **System security protocols:** Implementing security over system correspondences and incorporate HTTPS, SSL, and SFTP.

- **System the board protocols:** Provide network administration and upkeep and incorporate SNMP and ICMP.

3.2.3.1 Internet protocol (IP)

The Internet Protocol (IP) is a protocol, or set of rules, for steering and tending to bundle of information so they can traverse arranges and land at the right goal. Information navigating the Internet is isolated into little pieces, called bundles. IP data is appended to every bundle, and this data causes switches to send parcels to the ideal spot. Each gadget or area that interfaces with the Internet are relegated to an IP address (1). As parcels are coordinated to the IP address connected to them, the information shows up where it is required. When the bundles land at their goal, they are dealt with contrastingly, relying upon which transport protocol is utilized in mix with IP.

3.2.3.2 TCP/IP

The Transmission Control Protocol (TCP) is a transport protocol that directs how information is sent and received. A TCP header is incorporated into the information segment of every parcel that utilizations TCP/IP. Before transmitting information, TCP opens an association with the beneficiary (6). TCP guarantees that all bundles land all together once transmission starts. Using TCP, the beneficiary will recognize getting every bundle that shows up. Missing parcels will be sent again if the receipt isn't recognized.

TCP is intended for unwavering quality, not speed. Since TCP needs to ensure all bundles land altogether, stacking information using TCP/IP can take longer if a few parcels are absent. TCP and IP were initially intended to be utilized together, and these are frequently alluded to as the TCP/IP suite. Be that as it may, other vehicle protocols can be utilized with IP.

3.2.3.3 UDP/IP

The User Datagram Protocol, or UDP, is another generally utilized transport protocol. It's quicker than TCP; however, it is likewise less solid. UDP doesn't ensure all bundles are conveyed and all together, and it doesn't set up an association before starting or getting transmissions. UDP/IP is typically used for gushing sound or video (7). These are use situations where the danger of dropped bundles (which means missing information) is exceeded by the need to keep the transmission ongoing. For example, when clients view a video on the web, a few out of every odd pixel.

TCP and UDP carry network packets and These packets are just bits of records that journey over the internet.

Both TCP and UDP forward the records packets from the machine using ports to one-of-a-kind routers till they reach the final destination. They are additionally used to ship the packets to the IP address of the recipient. (An IP address is a special address assigned to every device connected to the internet.)

3.3 Network Security Threats and Vulnerabilities In SMEs

3.3.1 Network security

Firstly, there are some discussion about network security. Network security is special for SMEs. Small and medium-sized enterprise networks frequently experiencing random cyber-attack. There is no completely secure application, protocol, secure appliance, or network (8). A lot of new types of threats, vulnerabilities are discovering every day. Even the network monitoring system is affected, which is very smart to detect attacks. For many reasons, cybersecurity engineers who are finding security whole in the company network are highly paid.

3.3.2 Hackers

Hacker is a person who is accessing a computer without proper permission and stealing important and sensitive data from the system. Generally, one could say every hacker has very high skills computers. Based on their skill and attack type, hackers are can categorized (9).

3.3.2.1 White Hats

Ethical hackers are in the white Hats category. Ethical hackers are security experts who will systematically penetrate the computer network on behalf of its owner's permission and find security vulnerability. They are not attempting to attack another company network for money purposes (9). Companies are coordinate very closely when ethical hackers are testing or searching security whole.

3.3.2.2 Grey Hat and Black Hat

Gray Hat category hackers refer to a hacker who is not too mischievous or altruistic (2). Grey Hats are not consulting with companies for hacking, and it's the big difference between

White Hat and Black Hat. Grey hacker that will preserve all exploit data only for himself, but Black Hat will not. Black Hats are very Malicious users on the internet, and they do not have any Moral value. Black hackers are motivated by money, and generally, they break the security and steal, modify sensitive data. They are often called crackers by the network (10). Not only Online threats are popular. It can be discussed the Physical Security of the network.

3.3.3 Category of security threats

Nowadays, network security is becoming a most discussed topic because network treats are available. The small and medium-size enterprise network is not out of risk at all. A system delivered threats can be two types, which are Passive Network threats and active network threats. Based on a Microsoft security intelligence report, malware needs direct user interaction, and it is about 45 percent. Attackers are trying many ways to destroy the network security (6).There are four types of attack based on the “Network security Bible.

1. Modifications attack

2. DDOS attack (Denial-service attack)

3. Replication attack 4. Access attack

For specific instances mentioned, basic types of attack can be combined. Based on the existing technique, attackers get help to decide what type of attack vector they should choose, and it’s called port scanning.

Usually, security threat comes from two places.

- External user
- Internal user

External security threats happen when someone outside of the network creates a security threat for the web. If there is an instruction-detection system (IDS), it’s easy to determine these types of network security attacks. A shocking number of attacks happen every single day in our computer network. So, there is an urgency to follow some secrecy for the internal user (4).

3.3.3.1 Structured Threats

Structured threats happen when a technically skilled person is trying to gain access to our network. A hacker creates or uses some very sophisticated tools to break network security. For example, ICMP flood, it’s an excellent example of a structured attack (11). A less skilled hacker can create these kinds of ICMP floods from the same machine and track the desired machine.

3.3.3.2 Unstructured Threats

A structured threat is external threats, and these threats arise from a malicious individual or group of malicious individuals. Even it can be a malicious organization. A good network security solution easily creates a defense against these attacks. Many effective tools are available on the internet, which can be used to find the targeted network's weakness.

3.3.4 Network Security Attacks

3.3.4.1 Port scanning Attack

Port scanning is mostly used before the major attack because it helps attackers discover open ports and which application is running on the workstation. Attackers get help to decide to choose the attacking method for the targeted machine (6). Network administrators and penetration tester frequently use port scanning for improving security though this technique is considered malicious.

Detection of port scanning Attack

The network monitoring system can detect port scanning techniques. A network monitoring system sends the packet to a specific port on a host and analyzes responses to learn about detailed services. There are few port scanning methods such as NULL scan, Acknowledgement scan, SYN scan, etc. In the slow port scanning detection process, a Small-time window detects slow port scanning (12).

3.3.4.2 Trojan horse Adware and spyware

Trojan horse or trojan is a powerful malicious software. Hackers are using to gain user access to malicious activities such as stealing important and sensitive data. Computer network threats are improving their attacking quality so quickly. The especially Trojan horse has lots of updates. The basic purpose of malware is stealing data, so changing attacking types is based on the situation. Malicious spyware will infect the workstation and spy on the individuals using it. This malicious software typically features keystroke loggers that can be used to discover the password and other sensitive information (3).

3.3.4.3 Computer worms and botnet

The computer worms no need human interaction for spreading out to other workstations. Computer worms can replicate and spread so fast. Interestingly, Rootkits will take administration-level access to a computer network for malicious activity. Rootkits are equipped with password stealer, antivirus disabler, and so on. Rootkits distributions include a malicious link, downloading software from a harmful website (7).

Phishing has the goal to steal sensitive data from workstations like other malicious software. The attackers often come in the form of instant messaging. The mail is appearing, and it seems valid. When the recipient is opening a tricked email, that time workstation is infecting. They will ask about much personal information will be giving away.

3.3.4.4 Computer virus and rogue security software

A computer virus is the most popular network threat, and its pieces of software are designed to be spread from one system to another system so fast. A computer virus can come as an email attachment, or it can be downloaded from the website (13). Computer viruses are known to disable the existing security system sending spam and steal a password, valuable data from the workstation. Not only virus there are other frauds are very active on the internet like Rogue security software. The rogue Security software basically misleading users very smartly.

When Workstation is infected, users will believe a computer installed on their computer or their security system is not updated. And finally, hackers will suggest the user install their software for removing installed software on the workstation. In this case, installed software and suggesting software both are malware.

Many websites use SQL for storing data. Day by day, network security threats have advanced, and bad actors improve the target's tricks. SQL injection assaults are no longer new concepts. Hackers are designed to target-driven functions by using exploiting protection vulnerabilities’ uses malicious code to gain personal data.

3.3.4.5 Man-in-the-middle attacks

Man in the middle attack is not a new concept. It has a lot of definitions. The attacker hiddenly relays and changes communication between two real participants who trust and are directly communicating with each other. In simple words, participants will not understand someone is in the middle who is pretending to be a real participant. In the middle, man is very easy for unsecured communication such as HTTP and hard for secure communications like HTTPS (3). Sometimes attackers providing a malicious certificate to a participant for tacking control. This problem is easily correctable if there is the use of HTTPS and increases awareness for the end-user. Man in the middle attack isn't a contemporary concept and It has a lot of Mitigation.

- Make sure integrity of the user's workstation or devices
- Use proper and trusted certificate
- Increase security for the operating system (OS) and web browsers.
- Educating users about secure and safe network use.

Detection:

Man, in the middle attack, depends on what type of system being attacked. It's hard to detect in HTTP mode communication, which is not secure, and for HTTPS, all necessary checking will be done by the end-user web browser (12). A high-quality network monitoring system might help to detect this kind of attack when the routing pattern changed dramatically. Man, in the middle, the attack is a kind of combined attack to categorize it such as IP spoofing attack, Dos Attack. It can have a good defense if there is a network traffic monitoring system. It can be discovered many anomalies traffic by analyzing network traffic.

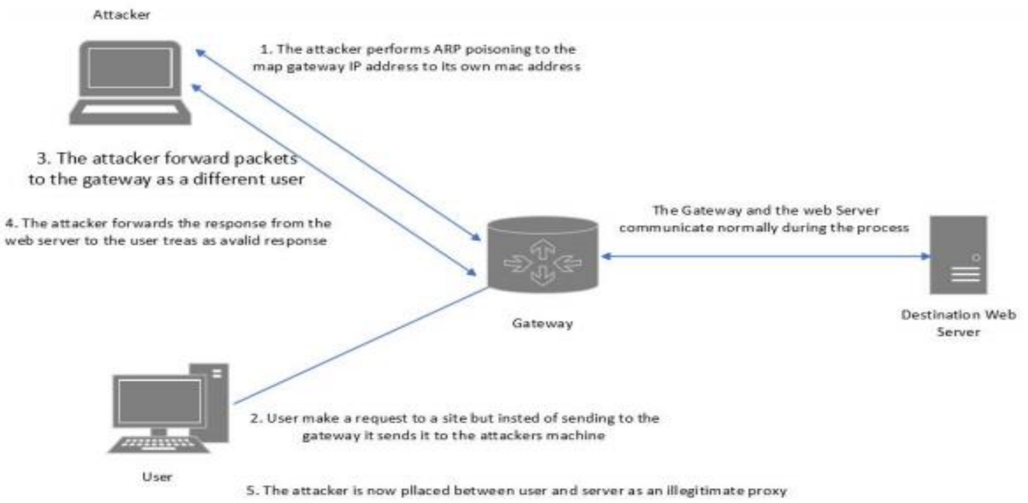

Attacker
1. The attacker performs ARP poisoning to the map gateway IP address to its own mac address
3. The attacker forward packets to the gateway as a different user
4. The attacker forwards the response from the web server to the user treas as avalid response
The Gateway and the web Server communicate normally during the process
Gateway
Destination Web Server
User
2. User make a request to a site but insted of sending to the gateway it sends it to the attackers machine
5. The attacker is now pllaced between user and server as an illegitimate proxy

Figure 03: Man-in-the-middle attacks

The attacker needs to understand

Every attacker has a specific target. For achieving the goal, the hacker wishes to get reply few solutions such as who is using the network, what is accessible, what the skills of the gear on the network are, when it's used least and most, and what is insurance place is. Malware nevertheless occupied the first role of cyber threat. Attackers are always using new methods such as avoiding old attacking vectors and hardware corruption; even hackers use visual basic instead of using Microsoft document (2).

Prevention:

- For protecting system need use Firewall and anti-malware software s
- When not sure about site and content, there is some risk to download files, attachment, and others
- Use only valid source of data
- Keep software up to date.

Detection:

Malware detection can be done by a Network monitoring application or cybersecurity software. And it will check incoming files or even rejected specific executable files. As malware does the malicious activity in the target workstation, it creates unusual behavior, even Outbound net flows (10).

3.3.4.6 Web-based attacks

Cybercriminals can be focused on when someone wants to achieve this objective web server and a web client. Bad URL is one of the main concerns, and it can have malware. A bad URL can redirect users to another unwanted page and its strong way to a victim user system.

Mitigation:

- Ensure protection of endpoints from unpatched software which containing vulnerabilities
- It should be avoided installing software via unknown third-party tools.
- Filtering incoming and outgoing web browser traffic.
- Keep updated and avoid unnecessary plugins of the browser.

Detection:

Web-based attack detection is achieved by a network monitoring system that uses many filters. The proposed URL from the User browser should check against a given list of malicious sites and a small number of web sites that are already detected as malware. It will be beneficial if there is a local list of malicious sites which are recognized by firewalls filters.

3.3.4.7 Cross-site scripting and Dictionary attack

The cross-site attack exploits vulnerable web application, and hackers set malicious script into a Web application. A dictionary attack is different from another attack, Cross-Site Scripting (XSS) attacks, and is a type of injection and its client-side code injection attacks. Scripts are injected into the trusted website, and this kind of attack happens when attackers use web applications to send lousy code. Most of the time, this script is a browser-side script (11). For example, an attacker could send malicious mail to a misleading user, and this email contains a link with malicious java scripts. If the user clicks those links, the user will be redirected to the malicious or unwanted website.

Cross-Site Scripting scripting vulnerabilities are a widespread issue for web applications. And fortunately, It can quickly be tested or examined company website or web application is vulnerable to XSS and other vulnerabilities by running a web scan. There are few tools such as "ACunetix "that can scan this issue. To keep a safe website from XSS, it's necessary to sanitize input. Application code should never be output data received. It is hard to trust any user input and need to use clean HTML (6).

A dictionary assault is a kind of approach of breaking the password of any laptop or server. Hacker systematically enters a word in a dictionary as a password, and this attack can be for data that is password protected and encrypted. Dictionary attack attacks have very close relations with brute force attacks. In brute force attacks, hackers all viable combinations of a password to achieve get entry to an account.

3.4 security solutions

3.4.1 Application Level Solutions

The security solution for the application-level is not similar. Different application has different level.

3.4.2 Authentication Level

Verification of any identity indicated validation or authentication. Authentication is a technique where the user can validate their status. Without proper information, the user cannot be logged in. Many traditional authentication processes are not suitable for a computer network Because a computer network carries sensitive data (6). There is some discussion about the essential authentication process.

3.4.2.1 Kerberos

Kerberos is an encryption and authentication service, and it is designed for using secret-key cryptography. Cisco router uses Kerberos to prevent data from being sniffed off. MIT designed Kerberos to protect network services and provide hefty security. Kerberos user authentication process is identical to RADIUS and TACACS +, and after authenticated, Kerberos granted something known as an admission ticket. By this admission, ticket user can (4).

Before Kerberos, Microsoft used an authentication technological know-how referred to as NTLM. NTLM stands for NT Lan Manager and is a challenge-response authentication protocol. The aim laptop or area controller mission and take a seem to be at the password, and shop password hashes for endured use.

The greatest distinction between the two structures is third-party verification and better encryption functionality in Kerberos. This greater step in the machine gives a massive extra layer of safety over NTLM.

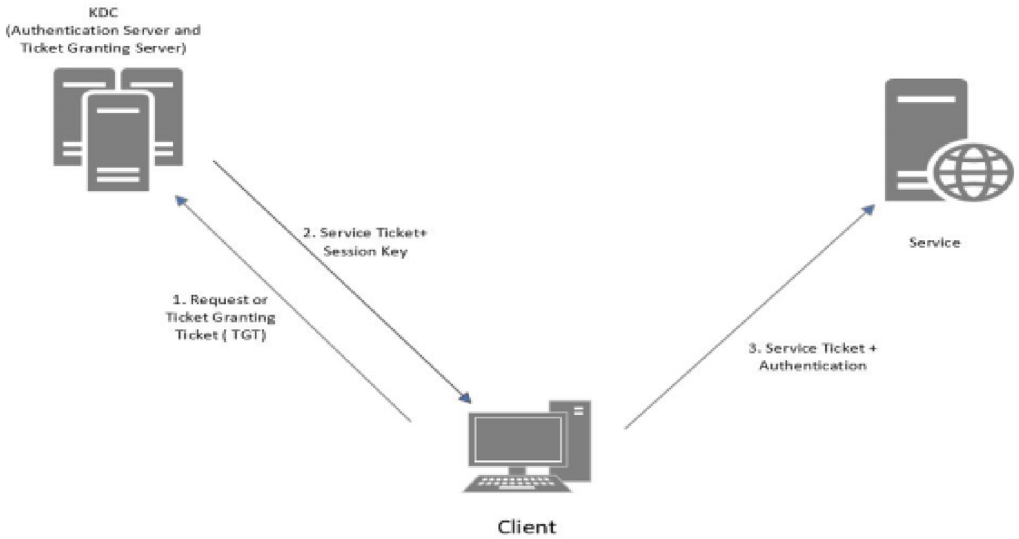


Figure 04: a simplified version of the Kerberos authentication system

Access other network resources without Their having to resubmit their credential. End devise to the router, Kerberos ensure encrypted communication. Virtual risks are not highly rated, and physical security is considered a high threat. It should not be crossed this point without ensuring proper security. Virtual security threats and physical security threats both are apparent (3). Physical security threat includes theft, human error, sabotage, and even environment disruption.

Another powerful authentication protocol called X.509 is based on the public key certificate, and this protocol is very widely used. S/MIME, IP security, and SET are excellent examples of X.509 protocol. The third-party can generate the public key, and it can false, so few risks are there. So, in this situation, there are some third parties who generate the public key with the certificate can be trusted. These certificates consist of user public keys (12). And these trusted third party called Certificate Authority (CA).

During SSL/TLS connections, the server authenticates by the handshake and file protocols. When initiating the handshake protocol, the server affords a signed X.509 certificate to the client. Only the server needs to be validated in most invulnerable shopping sessions. Client authentication is less common; however, it would require the server to confirm the client's certificate.

3.4.2.3 Secure shell (SSH)

Instead of using telnet, SSH can be used. SSH utility provides far off router administration with ample privacy. Secure shell (SSH) uses port 22, and an invulnerable shell gives similar functionality to an outbound telnet connection. Secure shell (SSH) ensures impervious conversation over an insecure network (1).

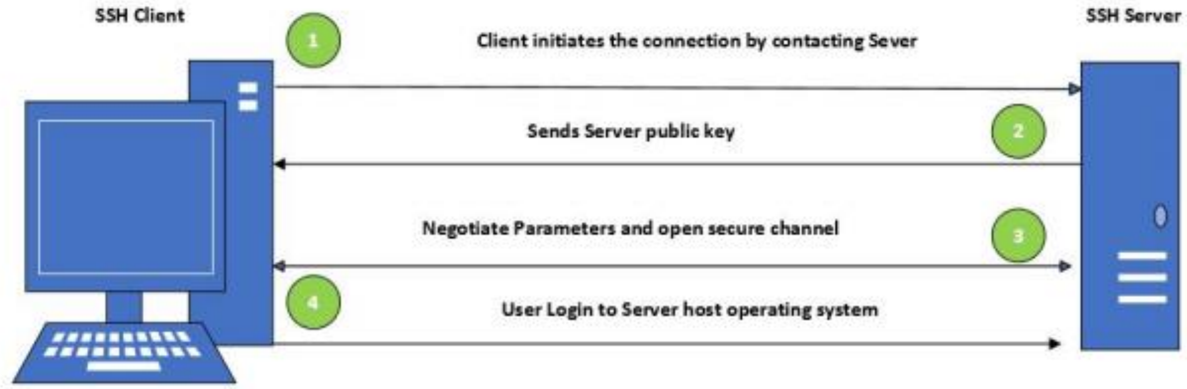

SSH Client
SSH Server
1
Client initiates the connection by contacting Sever
2
Sends Server public key
3
Negotiate Parameters and open secure channel
4
User Login to Server host operating system

Figure 05: SSH client-server handshake process

3.4.2.4 Remote Authentication Dial-In User Service (RADIUS):

Remote Authentication Dial-in User Service developed by Internet Engineering Taskforce (IETF). RADIUS is essentially a security system, and it prevents unauthorized access to the network. RADIUS is an open standard; that is why almost all vendors effort it (8). RADIUS is the most used security server, and it deploys client-server architecture.

RADIUS authentication process has 3 basic part

- Username and password request

- Username and complex password, which is encrypted, will be sent to the RADIUS server.

- Based on information match, the RADIUS Server will decide user should be Response, accepted, rejected, or changed.

3.4.2.5 Terminal Access Controller Access Control System (TACACS+)

Switch manages authentication of logon attempts with TACACS +via console port, and it's possible also using telnet. TACACS+ is security sever. RADIUS and TACACS + nearly the same, and TACACS+ is developed by the cisco system and can interact with the Cisco AAA service. Not only login and password authentication function, but also it supports a messaging system. When the user logged in, this security protocol can send user activity details of what the user is doing (14).

3.4.3 Email Level security solution

Electronic mail is not a new concept, and it’s the most widely used application across all platforms.

3.4.3.1 Pretty Good Privacy (PGP)

Philip R. Zimmermann developed Pretty Good privacy and its fantastic effort of a single man. Pretty right privateness (PGP) gives confidentiality and authentication provider email and even for file storage applications. There is some traditional encryption, which is quick primarily based on one key, and this key is used for both encryption and decryption This key's secrecy is very important, and there is only one big problem, which is the distribution of the key—single key distribution problems solved by public-key cryptography (5). There is use of two keys for public encryption and a private key used for decryption. So, anyone can encrypt data with the public key but only decrypt data which has a private key.

The public key can be risky, even though it seems very secure. Pretty Good Privacy (PGP) added a compelling extra feature for cryptographic schemes. When the user encrypts their data with Pretty Good Privacy (PGP) at that time, PGP compares the message and then creates a one-time secret key responsible for data encryption (15). Data encryption using Pretty Good Privacy (PGP) consists of five steps.

Authentication: When a user creates a message, which is a 160-bit hash code, the message is generated with the help of SHA-1. SHA-1 is a cryptographic hash function. When a user uses a private key, this hash code is encrypted with RSA. And the receiver recovers the hash code and decrypt it with the sender's public key (1).

Confidentiality: Pretty Good Privacy (PGP) provides full confidentiality by encrypting the data or message where CAST-128 IDEA and 3DES algorithms are used for encryption. In the beginning, the user generates a message with the 128-bit session key, and it's for one-time use. After, the message is encrypted with IDEA, 3DES, or CAST-128 algorithms. In the end, the user recovers data with the private key.

Compression: Good Privacy (PGP) compress the message after applying the signature, and it happens only before encryption. There one important fact, encryption happen before compression because more difficult to get their information from the compressed message. Here for compress the message ZIP algorithm, what can be used.

Email Compatibility: Good Privacy (PGP) use block consists of 8-bit octets, and many email systems allow ASCII text. Segmentation and Reassembly: The email message has its maximum length. To avoid this restriction, Good Privacy (PGP) breaks the message and sends it to the destination. Receiver end Reassemble that broken message and make it original, which is not broken.

3.4.3.2 Secure/Multipurpose Internet Mail Extension (S/MIME)

Multipurpose Internet Mail Extension (MIME) is defined differently, and it only accommodates the non-ASCII data. However, Multipurpose Internet Mail Extension (MIME) is not a mail transfer protocol, and it is the only extension of SMTP. When a body part is unstructured data, the header is responsible for message transmission. Multipurpose Internet Mail Extension (MIME) allows email to attach sound, picture, etc. Multipurpose Internet Mail Extension (MIME) has no security as it works as an extension of SMTP (5). Secure/Multipurpose Internet Mail Extension provides safety for Multipurpose Internet Mail Extension, and it makes use of a digital signature.

IP Level

Playing security on the Internet protocol (IP) level is very effective for securing communication for application.

Internet Protocol Security (IPsec)

IPsec is a set of algorithms, and it's not a single protocol. IPsec allows a unique entity to speak very securely with every other. Internet Protocol Security (IPsec) gives encryption and authentication to all at the internet protocol (IP) level. Internet Protocol Security (IPsec) has very strong cryptography (6). Authentication and data encapsulation are the two most basic parts of Internet Protocol Security (IPsec).

Encapsulation Security Payload (ESP) and Authentication Header (AH) are provided by IPsec, which are responsible for authentication and encapsulation.

3.4.4. Web Level

Web-level security is crucial as it's visible for everyone, and most users are not aware of the risks. Unauthorized remote access can be done when the server-side will have some misconfiguration.

3.4.4.1 SSL/TLS

There are few effective approaches for securing the web, and it has a different kind of applicability with the concern location in the TCP/IP protocol suite. There is one advantage of IPsec is that it is very clear to the end-user, and admin can filter the traffic. The secure socket layer (SSL) is the most common security mechanism which is available on the internet. The secure socket layer (SSL) is one kind of cryptography. Secure socket layer (SSL) version 3 and got TLS. TLS is more secure than SSL and its standard. TLS almost the same as SSLv3 and SSL/TLS encrypted data in the Transport layer. Normally, HTTP uses port 80, but when it is HTTPS that time, it uses port 443 for establishing a more secure connection. The secure socket layer (SSL) supporter browser can handle very sensitive data like credit card data (2).

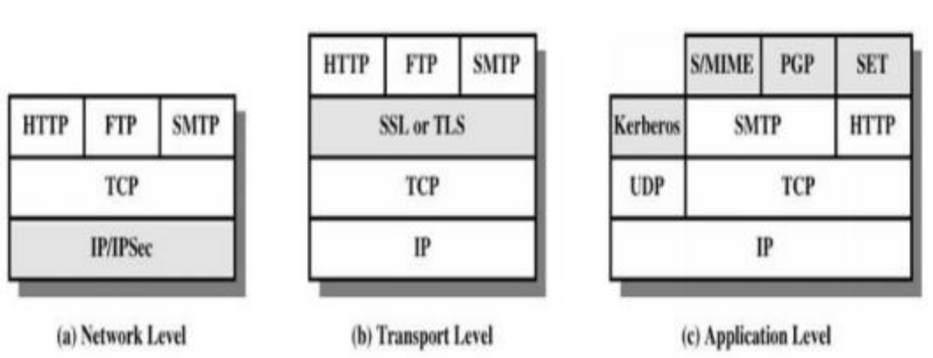


Figure 06: Security facilities in the TCP/IP protocol stack

3.4.5 System Level security Solutions

3.4.5.1 Intrusion Detection System (IDS)

This portion explains the IDS and modern method for network security analysis, and focus is the method working at the IP layer that means network layer. In the beginning, some

explanation has been provided about the basic term of Intrusion detection and traffic acquisition (2). It can be evaluated each method based on the following criteria:

i. Coverage
ii. Effectiveness
iii. Performance
iv. Application for many types of data acquisition
v. Ability to intrusion detection in encryption traffic

The first criteria are coverage, and it means the ability to find security threats. The coverage will be successful when both known and unknown cyber threats are detected. The next criterion is effectiveness, which indicates the accuracy of detection. And the 3rd one is performance, and it's very crucial because deployment is not easy in high-speed networks. And the ability to instruction detection in encryption traffic is most important nowadays network. Intrusion detection Based on position inside of the network, intrusion detection system (IDS) can be divided into two parts, which are Network-based intrusion detection system and host-based intrusion system (7).

Network-based intrusion detection system (NIDS): this type of intrusion detection serves the whole network or segment of the network where all inbound and outbound traffics are inspected for a suspicious pattern, which can be represented as a string of character signature. This certain type of pattern indicates a certain type of attack. Another type of detection It can be add here, which is anomaly-based detection (1). In IDS, false positive and false negative these two terms are frequently used

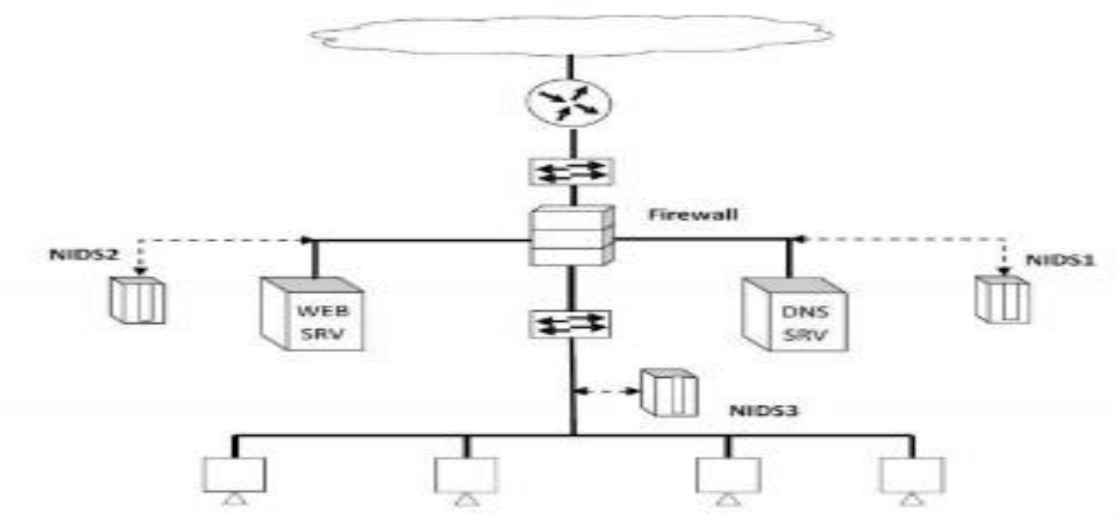


Figure 07: Network-based intrusion detection system-based network

Network interface card (NIC) card can communicate with other communication media such as media access card (MAC). The network interface card first creates an internet control message protocol (ICMP) request for acquiring an Internet protocol (IP) address. ICMP request is broadcasted inside the NIC network, and the ICMP request creates a change of network congestion as it is a bulk request. NIDS monitors all the identical types of instruction with the right network interface card. NIDS generates a log file (13). A network-based intrusion detection system (NIDS) has a feature to monitor all network switches. If NIDS finds any sign of intrusion, it will report about that instruction.

Host-based intrusion detection system (HIDS)

HIDS is a little bit extraordinary from a Network-based intrusion detection machine (NIDS). A host-Based Intrusion detection gadget (HIDS) can be mounted in one neighborhood machine. It is responsible for monitoring local system status such as CPU performance, file sharing resources, web server application, email service, etc.

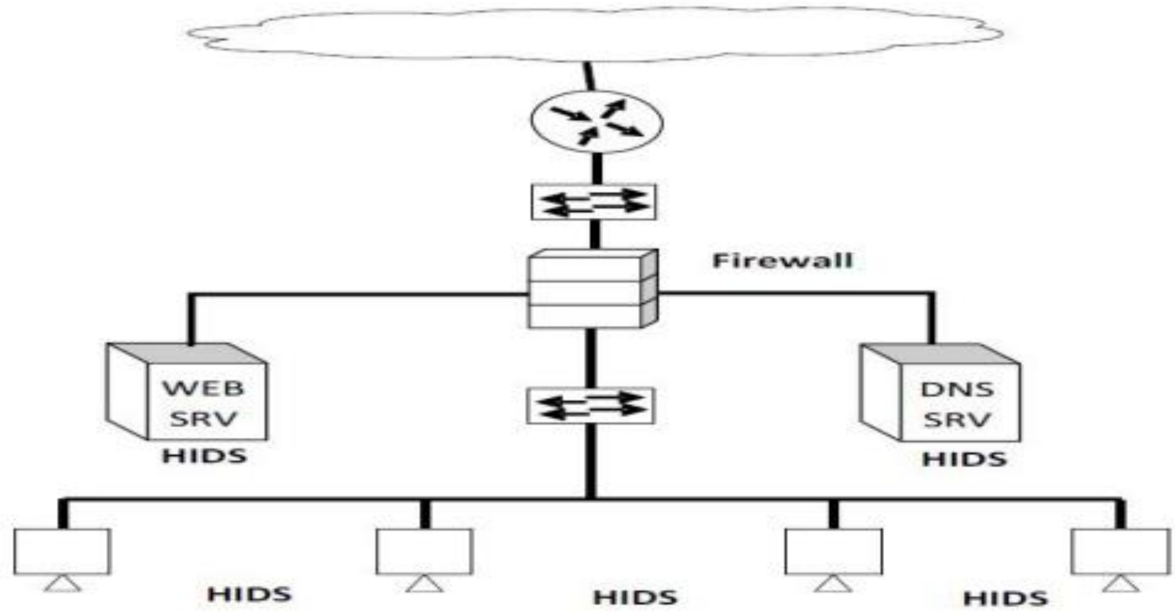


Figure 08: Host-Based Intrusion detection system (HIDS) based network.

3.4.5.2 Intrusion Prevention System (IPS)

An intrusion prevention system (IPS) is a reactive machine in which an Intrusion prevention machine is tightly brought with a firewall. The main task of the intrusion prevention system (IPS) is to stop identified cyber-attack. It can be Classified as the Instruction prevention system into three classes where are host-based, network-based, and another one has distributed intrusion prevention systems (IPS) (15).

3.4.5.3 Antivirus Techniques

There are many malicious applications/software that performs malicious activity within a workstation or on a network. These malicious applications can be a form of the virus, and this virus can infect or modify the system files or be from worms that may create their copy in a system and spread every weather. Few of them stay at the only local system, or some can travel from one machine to other machines through the network resources. Network resources can be a USB stick or CD/DVD etc. Antivirus technique is known as antivirus application or software. The functional architecture of Antivirus software is presented below.

Detection

Antivirus application can detect a virus or other malicious programs inside the system or data file, which is the first step that the Antivirus application does.

Identification

The second step is after detection malicious program Antivirus will be categorized, which type of virus and what virus want to do.

Removal

The last step is Antivirus software to remove the virus or malicious program from the system or machine.

Antivirus Functional Techniques

Few techniques are used by antivirus applications for detection, identification, and, finally, remove malicious viruses from the local system.

Generic Decryption (GD)

Generic decryption is an antivirus technique, and this technique is designed only for the polymorphic type of virus. The pleomorphic virus contains total encryption architecture and an encrypted virus signature. The generic decryption antivirus technique can detect and clean the type of virus which has polymorphic architecture.

Digital Immune System

The digital immune system or digital immune antivirus method gives protection against these sorts of malicious programs or viruses, which can unfold from one computer to another machine. It can be referred to here as worm because it can tour from one laptop to some other through a network.

The digital immune device has its own scanner elements for every customer machine, and each customer's laptop sends scanning records to the main administrator machine. Here administrator computer is a section of the same network. Administrator machines accumulate statistics and ship it to the virus analysis machine (12).

The virus analysis machine can be local or part of a wide area network. Here is one working block architecture for the virus analysis machine.

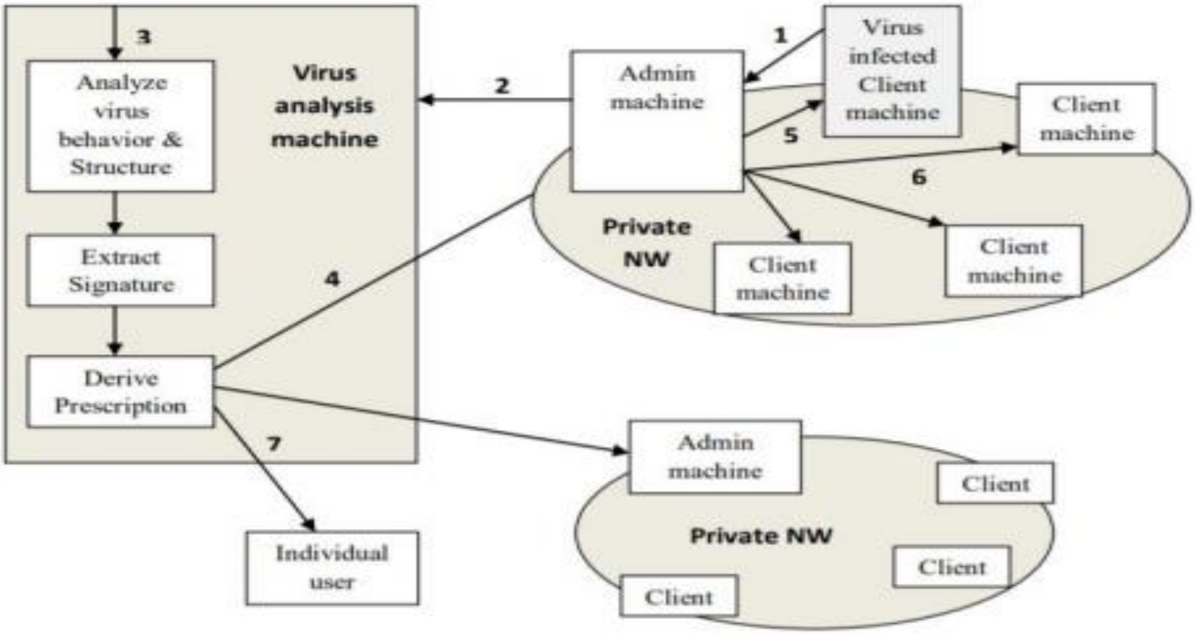
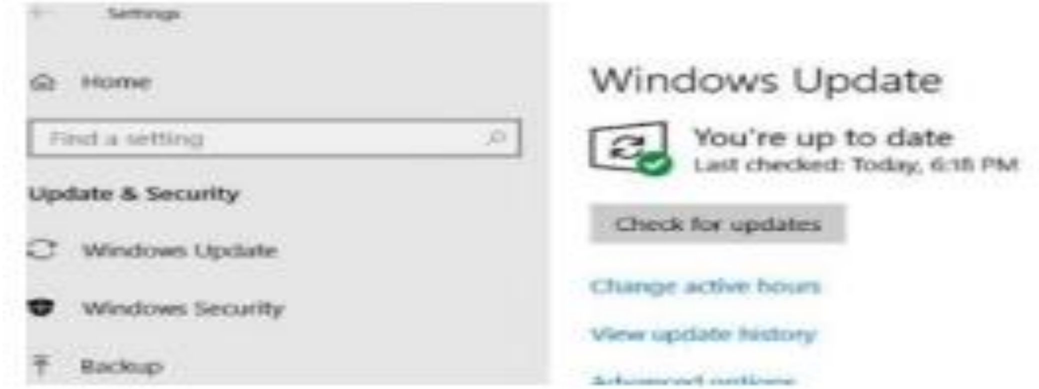


Figure 09: Digital Immune System

3.4.5.4 Workstation based security

The system administrator of on point followed a few steps to secure the workstation.

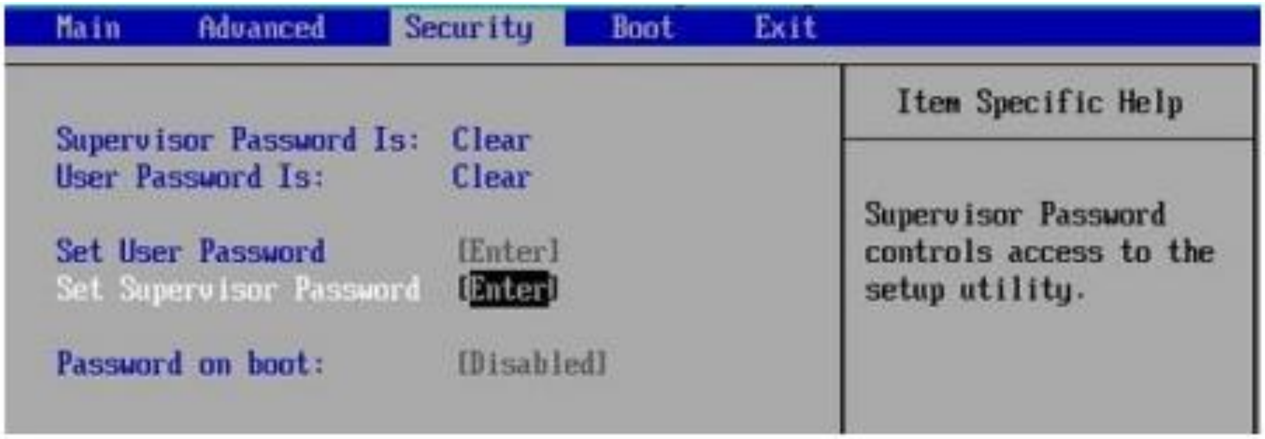
- Keep Operating system up to date.
- Antivirus software installed and keep up to date.
- Installed Anti-spyware software and keeping up to date
- A local firewall is an enabling mode.
- The strong password used for login
- Physical security such as cable and handy stuff is tied with a cable tie
- Removed unnecessary or less popular windows services
- BIOS password setting



You're up to date
Last checked: Today, 6:18 PM

Figure 10: Keep Operating system up to date

Microsoft routinely releases security updates because they try to keep their operating system secure from any security attack. Malware security holes are removed when OS gets a security update, so it is necessary to update windows.



Supervisor Password Is: Clear
User Password Is: Clear

Set User Password [Enter]
Set Supervisor Password [Enter]

Password on boot: [Disabled]

Supervisor Password controls access to the setup utility.

Figure 11: BIOS password setting

3.4.5.5 Firewall

A firewall is a network device which can isolate two different networks or system. The firewall decides what kind of traffic can pass through the web and what kind of traffic not, and the firewall decides the direction for network traffic as well.

A firewall is a network security device, and it provides properly defense in opposition to unwanted community traffic. The firewall may contain only one system or more than one (1). The primary role of a firewall inside the network protects one network from another network, and it must have two network interfaces for two systems. There are two interfaces of the firewall. One interface indicates the internal network, and another interface indicates an external interface.

Characteristic parameters: Firewalls follow few parameters

Service control

Firewalls manage those services which are valid for communication and control the communication service, which has extra-functional parameters such as source /destination IP address. Not only the IP address, but it can also manage service based on ports and types of the protocol as well.

Direction control

Firewalls can control user access behavior, and those users can be part of an internal or external network.

Behavior control

Network administrators can control firewall working behavior for a service and also for the user. The Administrator can grant access to the user (4). Access can give like full access/permission or partial access/permission. Simultaneously, the firewall can decide which user can be permitted for the specific service and which is not.

Types of firewall:

There are many kinds of firewalls in the market, and the Administrator can pick out which type of firewall is excellent for them. There are 4 types of firewalls packet filter firewall.

1) Application gateway
2) Circuit level gateway
3) Stateful filter firewall

Packet Filter Firewall

Packet filter firewall monitors all incoming and outgoing traffic based on a network packet. There is two option available. Based on the permission, the packet can be allowed or dined by the firewall. In this situation, the firewall compares with given parameters and then allows or dined packet. Packet filter parameters typically contain source and destination IP address, source /destination ports, and types of the packet such as TCP/UDP (4). When packet filtering happening a decision can be for a specific interface. Firewall rules can be set for inside and for outside interface. The packet filter firewall does not need a higher-level configuration for filtering. packet filter firewall is known as the first-generation firewall.

Application Level Gateway

An application-level firewall is more intelligent than a packet filter firewall, and it is of offers more shelter, reliability. The application layer firewall provides the best service on application layer traffic. It provides a client-server network environment. All client machines want to visit outside the network. That time firewall act as a gateway (16). All host act as a client and firewall act as a server.

Stateful Inspection Firewall

Stateful Inspection Firewall is a combination of a packet filter and an application-level gateway firewall. It can scan packet and application-level traffic. It ensures more security than other firewalls, and it’s called 3rd generation firewall.

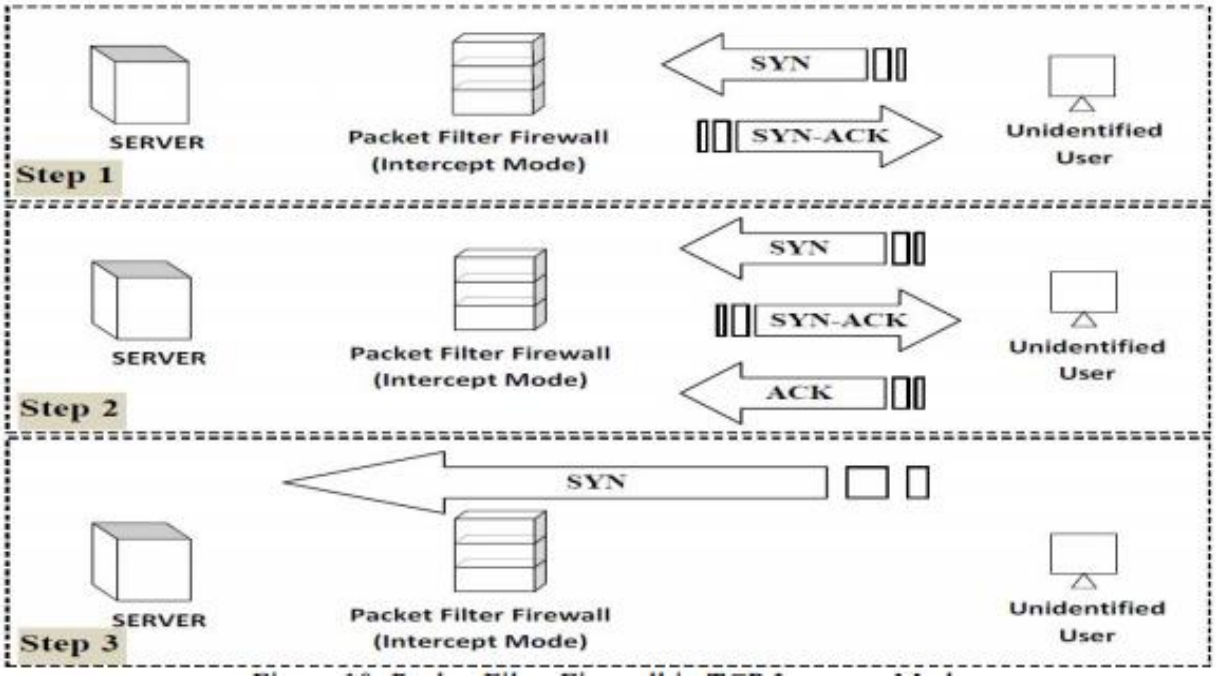


Figure 12: Packet Filter Firewall in TCP Intercept Mod

3.5 wi-fi network

An office network is significant for any business size, and each employee cannot work without a network. Employees can connect their smartphones, laptops, and tablets without a physical connection, so employees have greater mobility within the office. Most of the business use wi-fi network because it can be scaled very easily (10). As a result, they become more productive—the can-do lot of work. The internet is not a safe place at all. The wired network has many issues, but the wi-fi network also faces the same kind of threats. Business data need to be protected as employees are using wi-fi and wired network, so hackers target wi-fi networks also. So, it's so important to boost office wi-fi security.

3.5 .1 wi-fi network Security solution

Wi-fi networks are comparatively less secure than wired networks, and in wi-fi networks, unauthorized users can easily get access. Internet security threats are rising day by day. So not only wired network security, need to think, and ensure best security in the Wi-network. Basic wi-fi security provides a low level of security of the network.

3.5.2 Use stronger encryption

Few wi-fi access points provide Wired equivalent privacy (WEP) standard of protection. But hackers can break Wired equivalent privacy network using many hacking suites such as Air cracking within a minute. In this situation, it is essential to use some different Wired equivalent privacy (WEP) for wi-fi protected access, either WEP or WEP2 standard. It my practical to use wired equivalent privacy (WEP) with a pre-shared key for a small company and home.

Pre-shared key method indicates that all employee or family member uses an identical password for the connection. In this situation, network security depends on those users who desire employee and family members and are completely prohibited from sharing pre-shared keys with outsiders. Here is one good practice to change the pre-shared key when someone leaves the company. And periodically, it can be changed for security reasons. For a medium and large organization, WEP is in enterprise mode, which offers different user and password for each user (15). And it’s much easier to manage user profiles when an employee left the company. There is no hassle to change pre-shared keys.

3.5.3 Use a secure WPA password

There is some urgency to set a strong password that protects the wi-fi network. Strong passwords indicate that it has complexity, long enough and random, so it is hard to break for any hacker. In most of the cases, default access and setting are not changed, but it's not a good idea at all. Some settings need to change, which is set up as default because hackers' primary target is default settings.

After setting a wi-fi -a point, there should have a test about some vulnerability (5). Without revealing the password, it can be tried to break it using the Cloud Cracker service. The key mixing function creates a new key for every packet which needs to be transmitted, and it protects against RC4 weak key attacks.

3.5.4 Provide a separate network for guests

In company and home, there are a lot of visitors come every day and need to ensure internet access temporally. In this situation, It can be divided our company or home network for wi-fi access points. So, the guest user can get internet access without a company office or home internal network. This is very important for security reasons. Guest users are not able to spread the virus and not cable to do any malicious activity. for monitoring and controlling guest users, and It's good to set different SSID with a specific name.

3.6 Computer network monitoring system

Computer network monitoring is an essential part of computer network security. Network monitoring gives us visibility of the computer network, and network performance data can be collected, which is easy to read. When the network is down, that time is money. The professional network monitoring system can find the issue very quickly and based on the marked issue network administrator can fix it. That means employees can come back to work. Technology is changing. Professional network monitoring can provide valuable information to adopt updates. A professional network monitoring system can give us a history of all monitored instances.

Optimal Performance: The network monitoring system allows network administrators to optimize network performance by identifying the slowdown and problems area. Minimized Risk: The monitoring system can identify malicious behavior of the network, and this is the most significant benefit of the network monitoring system (17). The network monitoring system is responsible for keep track of network threats, unauthorized download, password changes, and so on.

3.6.1 Monitoring methods

Monitoring uses a different kind of method, and few are well defined. And rest of the monitoring method is not well defined, which means characteristics and behaviors are not well described. All characteristic of the monitoring method has a specific aspect. This subchapter described the direction of communication-based on methods, user's activity, logins, queries, and concern notification. The monitoring system is depending on the monitored entity and its data.

3.6.2 Characteristics of monitoring methods

It can be viewed as a first characteristic is the point of direction of communication, which differentiates between methods. Admin can categorize this method to push, pull, and push/pull. Here push methods describe that source is sending its specific data known or predefined destination. The pull method stores collected data locally. And the push /pull method does the same things together, which means it combines action. For example, SNMP uses the push/pull method because it is periodically pulling data from SNMP agents, and agents send data. Simple Network Management Protocol (SNMP) utilized a device that tells us the next characteristics of monitoring methods. The next characteristics are agent-based and agentless, and both monitoring methods have different criteria (11). Here agent is special software, and this software can listen to special events. These agents are placed very close to monitored entities and their activity as monitoring sources.

The Agent-base method also provides some extra features, such as data compression for better bandwidth utilization. Agent base can add extra security because it prevents unsecured communication. The main disadvantage of agent-based is needed to deploy it and main it. Another variation is an entity that notifies its state, or a client must query some sources to gather information. The query method periodically seeks information about the agent state. Here ping is the finest example of this query method. The network ping reveals the availability of the machine and round-tip time and number of hops. For example, if any incident happens, the machine is down that time, ping lets the montaging system know about the state changing. This state flipping is rapid, and it's hard to discover (9). This method not only best for problem finding but also to know for better insight. Notification method which is works differently.

3.6.3 Network monitoring

For network management, network monitoring provides necessary information. It's essential to discover community trends and analyze the issue. Network monitoring is the collection of statistics from the network for community management. network management applications are sending data, and the monitoring system is collecting those data.

Network monitoring indicates the monitoring of physical network gadgets such as routers, switches, firewalls, etc. and the network monitoring layer covers both the health and functional status of monitoring. Even though device health monitoring is the main concern in the hardware monitoring part. The device's health status is a part of the device log (5). Additionally, network traffic and performance of the network devices, network security-related events are also monitored. Data can be collected from SNMP agents belong to the network monitoring layer. And data can be obtained from intrusion detection systems (IDS) and intrusion prevention structures (IPS). Finally, the Network behavior system (NBA) provides data for network monitoring.

A network monitoring system should have some criteria, which are mentioned below.

- Monitoring of servers and workstations
- Identifying the scope and extent of monitoring
- Collecting and storing the data in a centralized manner
- Allow sharing the data with another system

3.6.4 Hardware monitoring

Hardware monitoring is another crucial part of the monitoring system, and it's responsible for device health and performance monitoring. Hardware monitoring directly checks the physical sensors of the devices, and it includes voltage, fan speed, the internal temperature of the equipment, etc. Few higher-level measurements such as CPU and CPU utilization input-output (I/O) speed, RAM uses, and so on (9). Besides, Hard disk failure events, hardware error rate, and SAMRT parameters are inside the Hardware monitoring.

3.6.5 Virtualization monitoring

Most of the SME computer infrastructure has a virtual machine because it's easy to manage and cost-efficient. This morning layer covers all software which is providing virtualization. And it can be in the could platform (AWS) or container platform (docker). Generally best example of collecting data about recourses metering and overall performance. In many cases, virtualization software requires a host OS to run on. And this host operating system is also included in the virtualization monitoring system. This Host operating system cannot be massive.

3.6.6 Virtual Infrastructure monitoring

Virtualized resources are monitored in this monitoring layer. It can be considered as virtual storage, virtual firewalls, virtual load balancers are virtualized resources. The monitoring system follows a basic principle which is already discussed before. Virtual infrastructure monitoring has different attention to the end-user and provider. For the user, it's simple monitoring of his or her virtualized infrastructure, for Infrastructure-as-a-service (Iaas) provider responsible for metering and billing. It can be less important and totally depends on cloud users and services.

3.6.7 Operating System monitoring

Entire workstations, laptops, physical and virtual machines are included and monitored in this monitoring layer. As per topics, this layer covers monitoring of the OS. Basically, logs or WMI, Syslog are monitored if it's Windows OS. If it's a Unix Operating system, few parameters will be different, such as monitoring the process and system recourse, which are the tread pool, ports files, system access, auditing, etc. And one more important thing is those Operating system (OS) used in host virtualization are not included in this section because it has some different role.

3.6.8 Subsystem monitoring

Subsystem monitoring is another critical part of the monitoring system. The subsystem portion includes a mail server, directory services, data processing framework, messaging engine. The subsystem monitoring responsible for taking care of these subsystems. The most basic way to monitor middleware is a log and other resource utilization. Based on middleware, it has specific uses. For example, an SQL analyzer can provide some hint about a situation, and a database has a metric that is easily accessible by SQL queries. If there is any docker container, all containers also will be included in the subsystem monitoring system. The virtual infrastructure monitoring layer and subsystem monitoring layer have a different focus on the provider of PaaS because of its service variation.

3.6.9 Application monitoring

The application monitoring layer is responsible for monitoring applications, Websites, API, etc. Here every single application produces a log, and the log can be analyzed for incident detection and prevention. This Layer covers error detection of applications based on analyzing logs. When an application is affected by a cyber threat, that time applications' normal behavior changes, and this kind of change is monitored by this layer.

This layer also covered application performance and utilization. If any website gets a huge number of requests, a new instance should take place . Unlike subsystem monitoring and operating system monitoring, the application monitoring system has a different kind of focus for the provider of the SaaS Cloud model.

Web server and application both need to be monitored in proper way. There are few metrics that should check for the webserver and its application. The key responsibility of a web server is accepting a request from a client and respond correctly. Application content can be static, dynamic, or other media. It should be concerned about a few things which are mentioned below.

- Requests received
- Appropriate response codes are generated
- Requested content is returned
- Latency is minimized
- Any errors and exceptions are appropriately handled

For server performance measurement, It needed to combine a few other metrics. These combine metrics determines how the server performs under different load environment. Server client relations can be transparent if admin check these things.

- Requests per second
- Bytes per second
- Bytes per request
- Uptime

And other infrastructure -a specific metric can be checked. Infrastructure -specific metrics such as CPU usage, memory usage, network bandwidth, Disk usage, and load can be added to the monitoring system for checking.

3.6.10 User monitoring

The user monitoring layer is the final layer, and for only the end-user. All data flowing inside the network are analyzed by the monitoring system, especially application behavior, the geographical location of the end-user (user position related to their workstation). It can be monitored Application utilization time and performance, planning, reporting, and another optimization. General data protection is significant because the user deals with their personal data—the user monitoring system monitors all these data and how it should be regulated.

3.6.11 Logging and log management

The most powerful technique of monitoring is generating and working with logs. The log is a kind of practice which are developed by developers. Interestingly, the log generates an important message that reveals the program operation's insight, behavior, and operating state. Logs are very important for this kind of software when it's developed and during production. Generally, the log has extract information about targeted monitoring. Software s should have a log because it is considered a best programming practice, which means every standard software should have a log.

Network devices such as routers, switches, applications, database servers, and access control systems have a huge data log. The main things are log is structured data, and It can be easily analyzed it. The main advantage of structured logs is easy to handle and troubleshoot. The main problem with the log is making a suitable structure. And sometimes, the log is overlocked and ignored by the system administrator the primary term log analysis, correlation, evaluation, and storage is known as log management. Log management is a basic and common method which is covered by every monitoring source.

4 Practical Part

4.1 Environment description

Onpoint s.r.o is a medium-sized IT company. Onpoint is developing finance-related software, Android apps, Games, and providing IT support. Onpoint s.r.o currently has 300 workstations, a small data center, and around 25 servers, and the number of servers is increasing based on time demand. Computers are grouped in logical groups, and it's called localities, which correspond to an organizational unit in the Active directory.

1. Classroom
2. Library or Study room
3. Working department

Classroom and Library used by Trainee of Onpoint s.r.o. All workstations in the classroom and library can be controlled remotely. The classroom is used by a student who is receiving technical teaching and a new joiner (employee). But the library is accessible for everyone for self-development study. Both localities have different kinds of software and security policies, which are maintained by the central management system. Computers of many working departments such as Human resource (HR), Customer support (CS), Finance, Developers, Design are using by an employee of Onpoint s.r.o. Every employee has their own workstation, and it has a basic set of software; if an employee wants special software, that time IT team responsible for the installation of that software.

4.2 Selected Technology And analysis

4.2.1 LAN Topologies

Even though there few topologies such as Bus, Ring, Star, and mesh are popular, the Network administrator selected Star topology for onpoit s.r.o.

Star topologies are the most frequent set up in a LAN. This is even more real in a minimal LAN, such as at home, pupil dormitory. This is because home, dormitory have their single centralized device, and all the other devices plug into that single centralized device. With Ethernet switches, the nodes physically connect to the switch as a star, and the logical flow of the traffic/data is also a star.

Star topologies are also super common in any other LAN. For example, there will be closet switches (aka access switches) where all the hosts/computers in that area plug into the centrally located switch. That is also a star topology, but how that closet switch is interconnected to the rest of the network switches may be using a different topology.

The Star topology is the most frequent, but it is not the best for redundancy, and thus, most corporate LAN infrastructures incorporate more redundancy into the overall network topology. So, corporate networks are a conglomeration of multiple topologies, and it can be found more than just a Star topology.

4.2.2 Ethernet

Ethernet describes how network devices can layout and transmit statistics. Other devices on the equal neighborhood or campus region community phase can recognize, get hold of, and method the information. An Ethernet cable is the physical, encased wiring over which the facts travel.

Connected devices getting get entry to to a geographically localized network with a cable that is, with a wired alternatively than wi-fi connection likely use Ethernet. From companies to gamers, numerous cease customers rely on the advantages of Ethernet connectivity, which consists of reliability and security.

Gigabit Ethernet and fast ethernet

Basis for Comparison	Fast Ethernet	Gigabit Ethernet
Basic	Offers 100 Mbps speed	Provide 1 Gbps speed
Delay	Generate more delay	Less comparatively
Coverage	Can cover distance up to 10 km.	Has the limit of 70 km
Relation	Successor of 10-Base-T Ethernet	A successor of fast Ethernet
Round trip delay	100-500-bit times	4000-bit times

Table 01: comparison between Fast Ethernet and Gigabit Ethernet.

In onpoint s.r.o LAN network, gigabit ethernet has been selected. Fast Ethernet is not faster than Gigabit Ethernet and provides maximum records pace up to a hundred Mbps. And the latter has elevated its pace at most to 1 Gbps by way of enhancing cabling technology, MAC layer, drift control protocols, and excellent service.

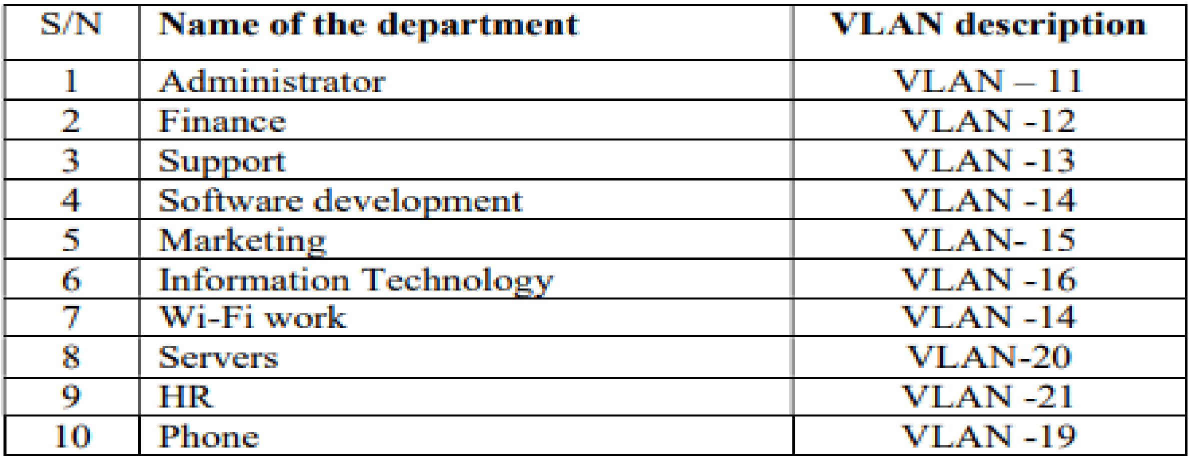
4.2.3 Onpoint s.r.o Network VLANs

In the network switches. Virtual Local Area Network (VLAN) technology is used. VLANs can unfold across multiple switches, with each VLAN being handled as its very own subnet or a broadcast domain. This skill that frames broadcasted onto the network will be switched solely between the ports within the same VLAN.

LANs (Virtual LANs) are logical grouping of devices in the equal broadcast domain. VLANs are commonly configured on switches using some interfaces into one broadcast area and some other interfaces. There are a few benefits offered by VLAN technology, which are mentioned below.

- Every VLAN has its very own broadcast domain, so VLAN will increase the quantity of broadcast domains whilst decreasing their dimension
- VLAN improves security as sensitive data can be placed on a separate VLAN.
- Using VLAN technology, users can be grouped based on department.
- Any changes to the network are easy; just a port can be placed in the desired VLAN.

There is ten VLAN in Onpoint s.r.o. Network. Here are the details.



S/N	Name of the department	VLAN description
1	Administrator	VLAN – 11
2	Finance	VLAN -12
3	Support	VLAN -13
4	Software development	VLAN -14
5	Marketing	VLAN- 15
6	Information Technology	VLAN -16
7	Wi-Fi work	VLAN -14
8	Servers	VLAN-20
9	HR	VLAN -21
10	Phone	VLAN -19

Table 02: Departments and VLANs

4.2.4 Virtual Private Network (VPN)

Internet Protocol Security (IPSec) and SSL VPN

IPsec is a Layer 3 VPN: For each network-to-network and remote-access deployments, an encrypted Layer 3 tunnel is established between the peers. An SSL VPN, in contrast, is typically a remote-access technology that affords Layer 6 encryption services for Layer 7 functions and, through neighborhood redirection on the client, tunnels different TCP protocols.

4.2.5 High availability (HA)

High availability (HA) is a deployment in which two firewalls are positioned in a crew, and their configuration is synchronized to stop a single factor of failure on company network.

Active-Active Mode

In this mode, each firewall is active, and so site visitors are load-balanced between each device, which is processing and filtering packets. If one firewall fails, the extraordinary firewall will take the full processing load till the failed firewall becomes energetic.

Active-passive mode

Like the active-active cluster configuration, an active-passive cluster also consists of at least two nodes. However, as they identify "active-passive" implies, now not all nodes will be active. For example, if the first node is already active in the case of two nodes, the 2d node has to be passive or on standby.

FortiGate firewall and HA (Active passive) for Onpoint s.r.o

In onpoint s.r.o network firewalls has configured Active-passive mode. Use an Active-Passive setup for a more resilient session failover environment. All traffic only goes through the Primary FortiGate unit. The Subordinate FortiGate unit(s) receives a replica of the Primary FortiGate unit's session desk and traffic. It remains in stand-by mode, ready to take over the Primary FortiGate unit fail. Active-passive HA presents session failover for most TCP, UDP, ICMP, multicast, and broadcast verbal exchange sessions. Active-passive HA does no longer supply session failover for conversation classes common through firewall insurance policies that include safety profiles. Active-Passive is more session failover resilient than Active-Active.

4.3 Networking devices

Onpoint s.r.o has a well-structured and secured network. In this network, few network components are installed, such as a router, switch, hub, firewall, etc.

4.3.1 Switch

The switch is a networking device used in the Access layer (Layer 2), and the switch can connect hosts that mean a workstation to a network. The switch can be defined as a network bridge with many posts that are responsible for the process and router packet at the data link layer.

Network switches become a primary target for hacking and leaking information. Information on the network is flowing to end-users to switch and then router. So, protecting switches against outside tampering is very important. The change makes use of a wired network to connect other devices using an ethernet cable. Network engineers of Onpoint s.r.o completed few steps for securing their network switches, which are described below.

Feature	**2960-XR**	**2960-X**	**2960-S**	**2960**
CPU	Dual core at 600 MHz	Dual core at 600 MHz	Single core	Single core
Stacking	FlexStack-Plus	FlexStack-Plus	FlexStack	No
Stack bandwidth	80 Gbps	80 Gbps	40 Gbps	-
Redundant power supply (RPS)	Yes	No	No	No
PoE+ 30W/port	Yes	Yes	Yes	No
Flash	256 MB	128 MB	64 MB	32 MB
Active VLANs	1K	1K	255	64

Table 03: comparison between cisco switches (2960-XR,2960-X ,2960-S,2960)

In onpoint s.r.o network, cisco 2960-XR switch has been selected based on exiting features and its clearly satisfy onpoint s.r.o network demand.

4.3.2 Router (ASA / FortiGate)

Most users do not know the ASA functionality and features, making it complex to operate Those turning to the ASA have a tendency to appear for a one-product, one-box solution and have to bother discovering it. There is news is that the ASA product line needs a faster operating system, cleaner interface, greater reporting structure, higher throughput, and more.

Both the Cisco ASA and Fortinet FortiGate safety furnish comprehensive visibility and advanced layer 7 security, hazard protection, intrusion prevention, net filtering, and software program control.

Feature	**ASA**	**FortiGate**
Throughput Range	up to 320Gbps	17Gbps - 1Tbps
Concurrent Connections	up to 60M	up to 320M
IPsec VPN Throughput	up to 51Gbps	up to 160Gbps

Table 04: Basic comparison between ASA and FortiGate

FortiGate 80F Series features

Features	**Capacities**
Firewall Throughput	10 Gbps
IPS Throughput	1.4 Gbps
NGFW Throughput	1 Gbps
SSL VPN Throughput	900 Mbps
Concurrent Sessions (TCP)	1,500,000
New Connections per Second	45,000

Table 04: Basic comparison between ASA and FortiGate

Firewall Throughput: 10 Gbps

IPS Throughput: 1.4 Gbps

NGFW Throughput: 1 Gbps

SSL VPN Throughput: 900 Mbps

Concurrent Sessions (TCP): 1,500,000

New Connections per Second: 45,000

Firewall Latency: 4 µs

Network Diagram of Onpoint s.r.o

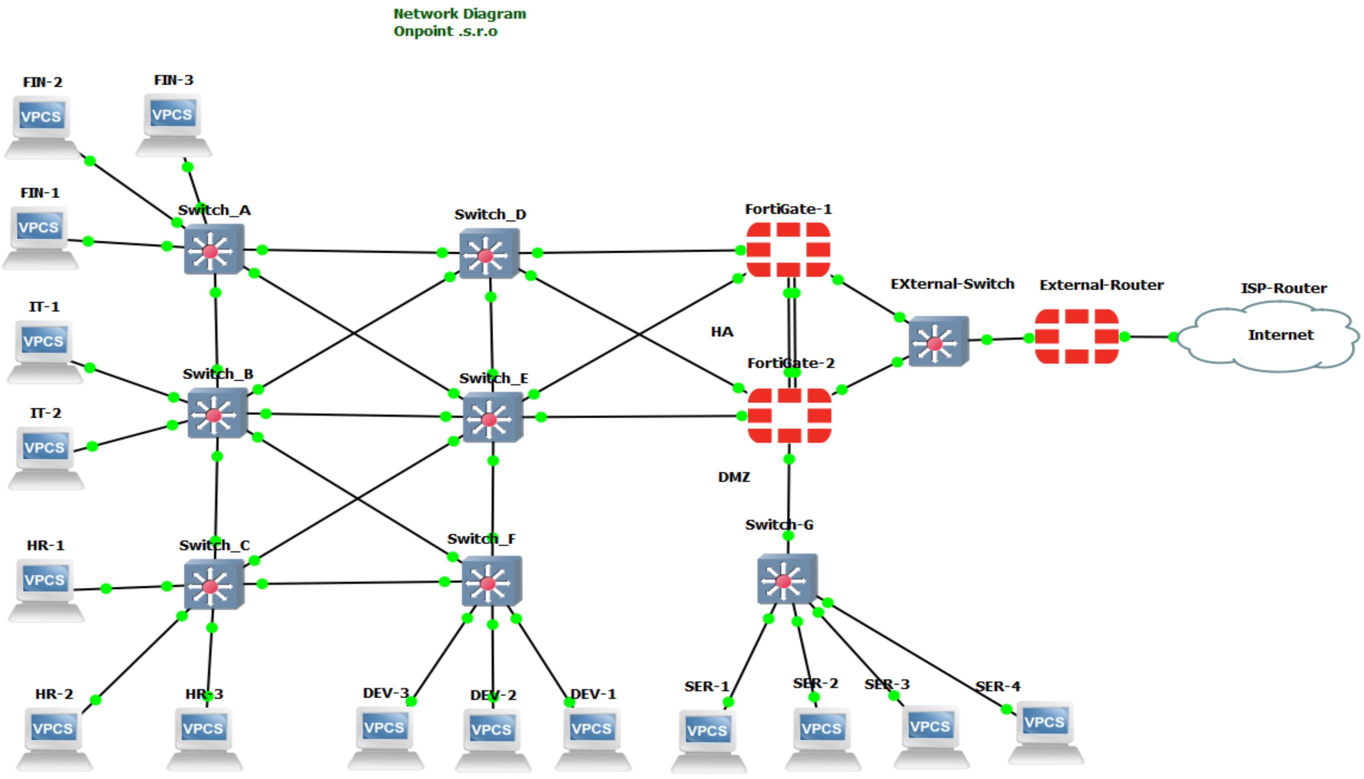


Figure 13**:** Network diagram of onpoint s.r.o

Onpoint s.r.o Office network diagram show the relationships between physical network devices such as Switches firewalls and few endpoints devices. In the network, all switches are cisco 2960-XR and there is two FortiGate firewall 80F has been set.

Local Area Network Diagram of Onpoint s.r.o

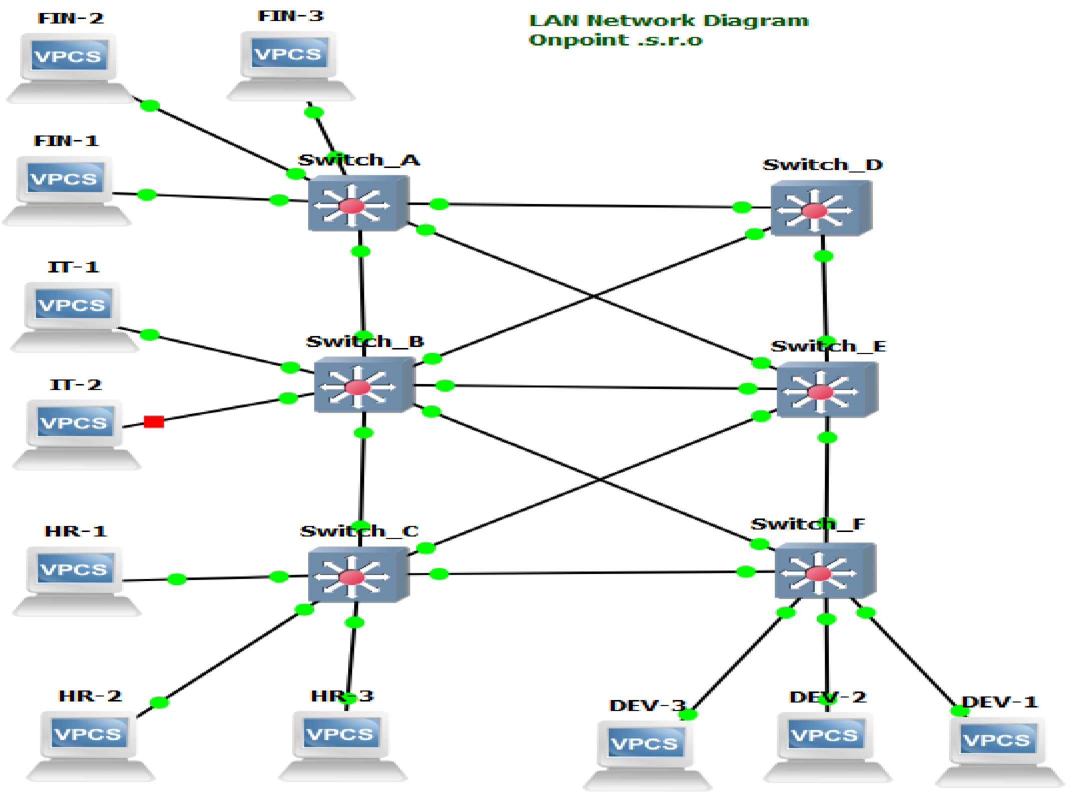


Figure 14: LAN diagram

4.4 Network switch configuration

4.4.1 Disable Dynamic Trucking

Switch VLAN share information via a Trunk link. Trunk, link use port, and that port called trunk port. Any ethernet port willing to convert as a trunk link. The administrator can do it manually, and its good practice—the network engineer of Onpoint s.r.o disabled dynamic Trucking in the switch for security reasons. The dynamic, which means auto, can carry network vulnerability.

4.4.2 Per VLAN Spanning Tree (PVST)

Per-VLAN Spanning Tree is a cisco proprietary spanning tree protocol. Each VLAN has its own STP, and the performance of the spanning tree per VLAN can perform better.
It reduces the CPU cycle for all the switches in the network. Per-VLAN Spanning Tree selects the root bridge automatically, and it optimized bandwidth usages.

4.4.3 Controlling Switch Access with Passwords and Privilege Levels

It can provide an additional security layer for a credential to cross the network or store it on a TFTP server. The administrator can use an enable password or enable secrete global configuration command. Administrators are deciding to set up enable secrete because it makes use of an elevated encryption algorithm.

4.4.5 Configuring Username and Password Pair

Username and password pairs are locally stored on the network switch. before getting access to the switch, they are assigned to the traces or ports and authenticate every user. For each username and password pair, the Administrator can assign a specific privilege level.

4.4.6 Password Recovery prevention

Network switch password can be recovered, and it can be done when someone has physical access to the switch. It's not good practice to provide access who is not a trusted person in the server room. Password can be recovered during the boot process, and anyone can interrupt the boot process and insert a new password. So, our recommendation is to disable this Password recovery mode.

4.4.7 Incidence management

If someone disables password recovery, it is recommended to keep a backup copy of the configuration file on a secure server in case the end-user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, Admin recommends that it's good to have a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, the Administrator can download the saved files to the switch by using the Xmodem protocol.

4.5 Router (FortiGate) configuration

4.5.1 Create an Enable Secret Password

Administrators need to create a strong "Enable secret" password because of its important part of granting privileged administrative access to the IOS. The administrator recommends long and complex passwords such as 10 characters long alphanumeric with social symbols.

4.5.2 Encrypt Passwords on the device

In onpoint s.r.o network admin have chosen password encryption for all network devices. Decrypted passwords can be unreliable, attacked/stolen by untrusted people.

All the credential which are configured in the cisco devices are represented as clear text in the configuration file, and administrator can change it. The administrator can make it unreadable, which means the admin can encrypt the clear text passwords using some commands.

4.5.3 Use an external AAA server for User Authentication

If admin use an external AAA server such as RADIUS or TACACS+, admin does now not need to create a local consumer account on each machine for administrator access. RADIUS or TACACS handles authentication, authentication, and accounting of user access to the devices. Network administrator cannot say something about an emergency, so it is very good practice to create one local user. If there is three network administrators, local account can be created for each admin. And as a result, it can be recognized which network admin acted. Local user account and it will be encrypted with MD5 hash so one could say it is secure.

4.5.4 Configure Maximum Failed Authentication Attempts

If there is a limit for maximum failed authentication login attempts, servers can avoid brute force password attacks. After crossing the limit user will be blocked automatically.

This is a significant part of the security for cisco network devices. The administrator can restrict IP addresses, which can SSH or Telnet, to network devices.

4.5.5 Enable Logging

For auditing, incident response, and monitoring, logging is very useful. The administrator can enable logging to an internal buffer of the device, and it can be done to an external log server. Log data is very helpful for performing analysis. There are 8 one-of-a-kind logging tiers (From zero to 7), and every stage affords steadily greater facts details.

4.5.6 Enable Network Time Protocol (NTP)

Enabling Network Time protocol (NTP) is essential for the previous section, which is about logging. And must have accurate and uniform clock settings on all network devices. Log data stamped with the correct time and time zone, and this helps us incredibly in incident handling and for proper log checking. Administrators have two options for enabling the NTP server. Administrator can configure an internal or external NTP server.

4.5.7 Secure Shell (SSH) configure

For command-line access to cisco devices, telnet is the default management protocol. All administration traffic is clear textual content with telnet, and that is why SSH is preferable as an alternative to Telnet. The administrator can configure SSH access to a Cisco network device.

4.5.7 Restrict and Secure SNMP Access

The simple network management protocol (SNMP) can be extremely helpful for collecting information from network devices. And it also has a security risk if it's not configured properly.

SNMP is, without a doubt, a very beneficial protocol for the management and monitoring of network devices, servers, and applications. Whether it is tightly closed or now not truly comes down to the change stage that is appropriate to the organization. SNMPv1 and v2c do have flaws in that authentication is almost non-existent. Where it is possible, constantly strive to use SNMPv3.

Some legacy devices, servers, and functions may have to be upgraded to help the more modern protocol.

Although SNMPv1 and SNMPv2 have same characteristics, 64-bit counters have been brought to SNMPv2, so it can also desire to assist faster interfaces. SNMPv3 replaces the simple/clear textual content password sharing used in SNMPv2 with greater securely encoded parameters. All editions run over the User Datagram Protocol (UDP).

Simply the use of SNMPv3 is now not sufficient to forestall abuse of the protocol. A safer method is to combine SNMPv3 with administration statistics base (MIB) whitelisting using SNMP views. This method ensures that even with uncovered credentials, facts cannot be examined from or written to the device except the information is wished for monitoring or everyday system re-configuration. The majority of gadgets that assist SNMP incorporate a widespread set of MIBs that are seller agnostic. This strategy permits the object identifier (OID) to be applied to devices regardless of manufacturer.

A hacker may abuse SNMP-enabled network units to get right of entry to an organization's network infrastructure. Here is some solution for SNMP abuse.

Configure SNMPv3 to use the easiest security handy on the device; this would be authPriv on most devices. authPriv consists of authentication and encryption features, and employing both aspects enhances basic network security. Some older pics may also no longer comprise the cryptographic characteristic set, in which case authNoPriv desires to be used. However, if the gadget does no longer aid Version 3 authPriv, it must be upgraded.

Ensure administrative credentials are suitably configured with extraordinary passwords for authentication and encryption. In configuring accounts, observe the principle of least privilege. Role separation between polling/receiving traps (reading) and configuring users or organizations (writing) is integral due to the fact many SNMP managers require login credentials to be stored on disk to get hold of traps.

It can be referred to vendor's guidance for implementing SNMP views. SNMP view is a command that can be used to restrict the handy OIDs. When OIDs are included in the view, all other MIB bushes are inherently denied. The SNMP view command should be used in conjunction with a predefined list of MIB objects.

5 Discussion

Result and discussion

OnPoint s.ro network is a security-focused network. In Local Area Network, Virtual LAN and demilitarized zone are configured. Based on Department VLANs are configured and its added extra layer of network security. Each VLAN has its own Subnet and its increased broadcast domain inside the network. VLANs reduces the security risks as the number of hosts which are connected to the broadcast domain decreases. The network is so fast as It can reduce congestion by sharing traffic as individual VLAN works as a separate LAN. And there is scope for future network expansion as well. Inside the network, there is a demilitarized zone (DMZ) is configured. The end goal of a DMZ is to enable a business enterprise to get right of entry to untrusted networks, such as the internet, whilst making sure its personal network or LAN stays secure. Organizations generally keep external-facing offerings and resources, as properly as servers for the Domain Name System (DNS), File Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and internet servers, in the DMZ.

The biggest advantage to a DMZ is in separating all unknown Internet requests to the servers on the DMZ and no longer permitting them into the LAN network. However, some additional advantages to deploying a firewall with a DMZ can help better recognize what happens in LAN and thereby increase security.

Onpoint s.r.o network has two firewalls that have HA configured. HA configuration, information has multiple paths from the source to the end-user. If one issue fails, statistics can traverse an alternate path. Therefore, with HA, It can be taken away single points of failure, guard against viable data loss, make sure to get the right of entry to modern data and reduce downtime.

OnPoint s.r.o network has its very own network monitoring system. Network monitoring is a quintessential IT manner the place all networking factors like routers, switches, firewalls, servers, and VMs are monitored for fault and overall performance and constantly evaluated to preserve and optimize their availability. One quintessential thing about network monitoring is that it ought to be proactive. Finding normal performance troubles and bottlenecks proactively help in figuring out troubles at the preliminary stage. Efficient, proactive monitoring can prevent Network downtime or failures.

Faulty Network devices have an effect on network performance. This can be eliminated through early detection, and this is why non-stop monitoring of the network and related devices is essential.

In positive network monitoring, the first step is to identify the devices and the associated overall performance metrics to be monitored. The 2d step is figuring out the monitoring interval. Devices like computers and printers are now not crucial and do not require standard monitoring, whereas servers, routers, and switches operate enterprise vital duties but at the equal time have specific parameters that can be selectively monitored.

Onpoint s.r.o has a Wi-Fi network, which is also network security focused. All Wi-Fi Access point has encryption enable with a strong password and disabled remote access.

In the practical part, there is explanation about few things which are on point. s.r.o network. In that network security designed by administrators, and they decided and deployed few import things such as they provide priority to endpoint machine security, network devices such as a router, switch hub, etc. security. And for all of them, they have a professional monitoring system for monitoring what is happening inside their network. They have a good opportunity to read logs that are generated by network devices inside their network. The professional monitoring system generates an alert based on attacks and sends those alerts to the administrator. Administrators are always very alert, and they are fixing network issues very quickly. So, they have a minimum amount of downtime in their network. As a result, employee, the services of the company are online. That is why the computer network of any company is directly connected with their productivity and profit.

Not only do administrators have the responsibility to maintain the security of the network, but employees also have a lot of work, which may help to secure the network. Training can be mandatory for employees on how to use their workstation properly. They can add awareness, which may help to build a very secure network, which is good for fighting against network threats. Though security attacking patterns are changing so fast, but there is some hope about skipping these unwanted issues.

Onpoint s.r.o Network administrator is security-focused as true network protection helps groups minimize the threat of failing victims of information theft and sabotage.

6 Conclusion

Onpoint s.r.o network is designed based on network security. Inside the network, all devices are very convenient for medium-sized enterprise office. The onpoint s.r.o network is focused on security as Small and medium-sized enterprise companies are known to flourish in today's economy. Companies are communicating with their client's daily basis. Company and customer relations are strongly related to their type of communication.. Nowadays, the internet is everywhere. So, most of the business is directly connected to the internet. Companies are sharing their product information via the internet. Company sales depend on spreading the news to the customer. SME needs a more secure network where they can share their valuable information with their customer. Today's internet is not a safe place at all. Threats. Hackers are waiting everywhere for malicious activity. One of the significant challenges for the company is securing its computer network, and they need it for more profit. Network administrations are always busy fighting with network security threats.

The main aim of this thesis used to be to discover network vulnerabilities for small and medium-sized corporation computer networks and in-depth analysis of network safety attacks. network security, not about a specific branded firewall and operating system. Adequately configured firewalls can protect against a lot of threats. Using a strong password and Antivirus can add an extra security layer. Periodically change passwords, setting a secure password, and updating Antivirus is good security practice. Adequately configured devices are essential, and it's better to have no security devices instead of incorrectly configured security devices. Network monitoring is vital for fighting against cybersecurity threats. The monitoring system can monitor the number of high-profile attacks. A sound network monitoring system provides alerts about malicious activity. So, system admin and network engineers can act quickly based on monitoring system alerts.

There was some observation in the simulation part, how to secure workstations and network devices. Others service such as Active Directory, Antivirus provide security in a computer network. Best security practices on network devices such as switches, and routers have been described in the simulation part. The network administrator configured the RADIUS server, and the RADIUS server provides authentication service. There is a bottom line that a network cannot be 100 percent secure as cyber-attack and other malicious activities are changing their attacking pattern. A reliable review will help to find out vulnerabilities in the system. It can be considered network analysis as a baseline of network security.

7 Bibliography

1. *Cryptology and Network Security.* **Lin, D., Tsudik, G. and Wang, X.** Sanya, China : in Proceedings of 10th International Conference on Cryptology and Network Security, 2011.

2. *Cisco networking essentials.* **Troy.** Indianapolis, Indiana : Sybex, 2015, Vol. 2. ISBN 1119092159.

3. **KÁLLAY, Fedor and Peter PENIAK.** *Computer networks and their applications : LAN / MAN / WAN.* Praha : Grada, 2003. ISBN 80-247-0545-1.

4. *Computer networks.* **Literature KUROSE, James F.** Brno : Computer Press, 2014. ISBN 978-80-251-3825-0.

5. *Computer intrusion detection and network monitoring: a statistical viewpoint.* **MARCHETTE, David J.** New York : Springer, 2001. ISBN 0-387-95281-0.MCMILLAN, Troy..

6. *Interconnecting Cisco network devices.* **MCQUERRY, Steve.** [ed.] 3. Indianapolis, Indi : Cisco Press, 2008. ISBN 1587054639.

7. *Network Routing and Switching.* **ODOM, Wendell, Russian HEALY, and Naren MEHTA.** Brno : Computer Press, 2009. ISBN 978-80-251-2520-5.

8. *Network Security.* **NORTHCUTT, Stephen.** Brno : CP Books, 2005. ISBN 80-251-0697-7.

9. *Computer Network Monitoring and Supervision System: System for Monitoring and Supervisory of Computer Network.* **MÍČA, Pavel and Roman TRCHALÍK.** Brno : Technical University, Faculty of Information Technology, 2008.

10. *Simulation In Computer Network Design And Modeling* . **H, Al-Bahadili.** Hershey : Information Science Reference, 2012.

11. *Simulation in computer network design and modeling: use and analysis.* **AL-BAHADILI, Hussein.** Hershey : Information Science Reference, 2012. ISBN 9781466601932.

12. *Introduction to computer and network security: navigating shade of gray.* **BROOKS, R. R.** Boca Raton : CRC Press, 2014. ISBN 978-1-4398-6071-7.

13. *Hacker proof: Your Computer, Your Network, and Your Internet Connection - Is It Really Secure?* **KLANDER, Lars.** Brno : Your Network, and UNIS Publishing, 1998. ISBN 80-86097-15-3.

14. *Computer networks.* **KUROSE, James F. and Keith W. ROSS.** Brno : Computer Press, 2014, 2014. 2014. ISBN 978-80-251-3825-0.

15. *Computer intrusion detection, and network monitoring: a statistical viewpoint.* **MARCHETTE, David J.** New York : Springer, 2001. ISBN 0-387-95281-0.

16. *Wireshark and Ethereal: a complete guide to network analysis and diagnostics.* **OREBAUGH, Angela.** Brno : Computer Press, 2008. ISBN 978-80-251-2048-4.

17. *Information and network security.* **SORIANO, Miguel.** Prague : Czech Technical University, 2013. ISBN 978-80-01-05297-6.

18. *The handbook of computer networks: distributed networks, network planning, control, management, and new trends and applications.* **The handbook of computer networks: distributed networks, network planning, control, management, and new trenEditor Hossein BIDGOLI.** Hoboken : Wiley, 2008. ISBN 978-0-471-78460-9.

19. *Basic network theory: with computer applications.* **VLACH, Jiří.** New York : Van Nostrand Reinhold, 1992. ISBN 0-442-00900-3.

20. *Cisco Network Security: Authorized Self-Study Tutorial.* **WENSTROM, Michael J.** Brno : Computer Press and Cisco Systems, 2003. ISBN 80-7226-952-6.

8. Appendix

Hostname setting

```
Switch>
switch# configure terminal
switch(config)# hostname switch-A-DT
switch-A-DT (config)#
switch-A-DT # copy running-config startup-config
```

Login banner settings

```
switch-A-DT (config)# banner login $ Authenticated user only! $
```

Configuring vlan using Config-vlan mode

```
switch-A-DT (config)#vlan11
switch-A-DT (config-vlan)#nameAccounting
switch-A-DT (config-vlan)#exit
switch-A-DT (config)#intfa1/0
switch-A-DT (config-if)#switchport mode access
switch-A-DT (config-if)#switchport access vlan 11
switch-A-DT (config-if)#end
switch-A-DT # copy running-config startup-config
```

4.2.1.1 Disable Dynamic Trucking

```
switch-A-DT (config)# interface type slot/port
switch-A-DT (config-if) # switchport mode access
```

4.2.2.2 Per VLAN Spanning Tree (PVST)

```
switch-A-DT (config)# spanning-tree mode rapid-pvst
```

4.2.2.3 Controlling Switch Access with Passwords and Privilege Levels

```
switch-A-DT >enable
switch-A-DT #configure terminal
switch-A-DT (config)#enable password onpoint!@#@#$123
switch-A-DT (config)#enable secret onpoint!@#@#$123
```

```
switch-A-DT (config)# service password-encryption
switch-A-DT # copy running-config startup-config
```

To see o enable passwords in configuration, use the following command:

```
switch-A-DT >enable
Password:
switch-A-DT #show running-config | include enable
enable secret 5 $1$BSX4$FZp.ZFvYSAGUEDn8dvr140
enable password onpoint!@#@#$123
```

4.2.2.4 Terminal Line Telnet Configuration

Telnet Password for a Terminal Line

```
switch-A-DT > enable
switch-A-DT # configure terminal
switch-A-DT (config)# line vty 0 15
switch-A-DT ng-line)# password abcxyz543
switch-A-DT Switch# show running-config
switch-A-DT # copy running-config startup-config
```

4.2.2.5 Configuring Username and Password Pairs

```
switch-A-DT > enable
switch-A-DT # configure terminal
switch-A-DT (config)# username Adam sample privilege 1 password secret456
switch-A-DT (config)# username 111111111111 mac attribute
switch-A-DT (config)# line console 0
switch-A-DT (config-line)# login local
switch-A-DT config)# end
switch-A-DT # show running-config
switch-A-DT # copy running-config startup-config
```

4.2.2.6 Password Recovery prevention

```
switch-A-DT > enable
switch-A-DT # configure terminal
switch-A-DT (config)# system disable password recovery switch all
```

```
switch-A-DT (config)# end
switch-A-DT # copy running-config startup-confi
```

4.2.2.7 Incidence management

4.2.2.1 Create an Enable Secret Password

```
Router-B-DT# config terminal
Router-B-DT (config)# enable secret MaDRaTCaT1234$#@yuh
```

4.2.2.2 Encrypt Passwords on the device

```
Router-B-DT # config terminal
Router-B-DT (config)# service password-encryption
```

1.2.2.3.1 RADIUS configuration

RADIUS configuration

```
Router-B-DT # config terminal
Router-B-DT (config)# enable secret K6dn!#scfw35
Router-B-DT (config)# aaa new-model
Router-B-DT (config)# aaa authentication login default group radius enable
Router-B-DT (config)# radius-server host 192.168.1.10
Router-B-DT (config)# radius-server key ‘secret-key’
Router-B-DT (config)# line vty 0 4
Router-B-DT (config-line)# login authentication default
Router-B-DT (config-line)# exit
Router-B-DT (config)# line con 0
Router-B-DT (config-line)# login authentication default
Router-B-DT (config-line) #end
Router-B-DT (config)#end
Router-B-DT # copy running-config startup-config
```

4.2.1.4 Create separate local accounts for User Authentication

```
Router-B-DT # config terminal
Router-B-DT (config)# username munir-admin secret Lms!a2eZSf*%
Router-B-DT (config)# username david-admin secret d4N3$6&%sf
Router-B-DT (config)# username pavel-admin secret 54sxSFT*&(zsd
```

4.2.2.4 Configure Maximum Failed Authentication Attempts

```
Router-B-DT # config terminal
Router-B-DT (config)# username john-admin secret Lms!a2eZSf*%
Router-B-DT (config)# aaa new-model
Router-B-DT (config)# aaa local authentication attempts max-fail 5
Router-B-DT (config)# aaa authentication login default local
```

4.2.1.6 Restrict Management Access to the devices to specific IPs only

4.2.2.5 Enable Logging

```
Router-B-DT # config terminal
Router-B-DT (config)# logging trap 6
Router-B-DT (config)# logging buffered 5
Router-B-DT (config)# service timestamps log datetime msec show-timezone
Router-B-DT (config)# logging host 192.168.1.2
Router-B-DT (config)# logging source-interface ethernet 1/0
```

4.2.2.6 Enable Network Time Protocol (NTP)

```
Router-B-DT # config terminal
Router-B-DT (config)# ntp server 1.1.1.1
Router-B-DT (config)# ntp server 2.2.2.2
```

4.2.2.7 restrict IP address

This is very important part of security for cisco network devices. Admin can restrict IP address which can SSH or Telnet to network devices.

Assume that the administrators' subnet is 192.168.1.0/28

```
Router-B-DT # config terminal
Router-B-DT (config)# access-list 10 permit 192.168.1.0 0.0.0.15
Router-B-DT (config)# line vty 0 15
Router-B-DT (config)# access-class 10 in
```

4.2.1.9 Secure Shell (SSH) configure

```
Router-B-DT # config terminal
Router-B-DT (config)# hostname Prague
Prague (config)# ip domain-name mydomain.com
Prague (config)# ip ssh version 2
Prague (config)# crypto key generate rsa modulus 2048
Prague (config)# ip ssh time-out 60
Prague (config)# ip ssh authentication-retries 3
```

4.2.2.8 Restrict and Secure SNMP Access

```
Router-B-DT # config terminal
Router-B-DT (config)# access-list 11 permit 192.168.1.0 0.0.0.15
Router-B-DT (config)# access-list 12 permit 192.168.1.1
Router-B-DT (config)# snmp-server network Cbd43@#w5SDF RO 11
Router-B-DT (config)# snmp-server network Xcv4#56&454sdS RW 12
```