Small Business Network Design with Secure E-commerce Server

A COURSE PROJECT REPORT

Submitted by

N S S S RAJA RAM PULAVARTHI [RA2111030010146]
CHIMMIRI PAVAN KALYAN [RA2111030010147]
MATSA BHARGAV [RA2111030010153]
CHUNDURU DHEERAJ [RA2111030010182]
SANNAPU VARUN REDDY [RA2111030010184]

Under the Guidance of

Dr. Arun A

(Assistant Professor, Department of Networking and Communications)

In partial fulfilment for the Course of

18CSS202J - COMPUTER COMMUNICATIONS

in

COMPUTER SCIENCE ENGINEERING
with specialization in CYBER SECURITY

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR - 603203

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that 18CSS202J minor project report titled “Small Business Network Design with Secure E-commerce Server” is the bonafide work of N S S S RAJA RAM PULAVARTHI (RA2111030010146), CHIMMIRI PAVAN KALYAN (RA2111030010147), MATSA BHARGAV (RA2111030010153), CHUNDURU DHEERAJ (RA2111030010182), SANNAPU VARUN REDDY (RA2111030010184) who carried out the minor project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE	**SIGNATURE**
Dr. Arun A Assistant Professor Department of Networking andCommunications SRMIST – KTR.	**Dr.Annapurani Panaiyappan K** Professor and Head Department of Networking andCommunications SRMIST – KTR.

TABLE OF CONTENTS

TITTLE **PAGE**

Introduction:

- The computer network infrastructure is the backbone of the business. All your devices, application, software and most of your work is supported by or built upon your computer network.
- To build a computer network for the company, you need to be quite careful as making a computer network run efficiently in a business environment is very different from setting home or domestic network.
- As we are dealing with 100 users, we will use LAN as our type.
- Many businesses have come to the realization that, in order to compete in the market, key business processes need to be part of the Internet. E-commerce has become a popular adaptation for businesses, which has been a major transformation for many businesses. The popularity of the Internet has transformed traditional commerce into e-commerce, which has proven to be a successful platform for many businesses. Small businesses provide an easy target for attackers because they typically have limited funds and do not have dedicated personnel to monitor, update and defend their systems. The attacks on small businesses continue to rise each year.

Abstract:

Small business e-commerce websites make an excellent target for malicious attacks. Small businesses do not have the resources needed to effectively deal with attacks. Large and some mid-size organizations have teams that are dedicated to dealing with security incidents and preventing future attacks. Most small businesses do not have the capabilities of dealing with incidents the way large organizations do. Security of e-commerce websites is essential for compliance with laws and regulations as well as gaining and maintaining the trust of consumers, partners and stakeholders. Many security standards have been established by various organizations to help guide security of small business servers, however, many of those standards or guidelines are too costly or time consuming. This paper1 will discuss how attacks are carried out and how a small business can effectively secure their networks with minimum cost. In points abstract for our project is:

- The aim of this project is to create a small-scale computer network design for a small business.
- The organization hosts an e-commerce website on a server.
- This website is accessible to users using http and public ip addresses.
- The network is designed with necessary hardware and software components

Existing system:

A small business network design with a secure e-commerce server typically involves several components working together to provide a secure and reliable environment for conducting online transactions. These components may include:

- Network infrastructure: This includes the hardware and software components necessary to establish a network, such as routers, switches, firewalls, and network cables.

- Web server: This is the computer that hosts the e-commerce website and manages the transactions between the customer and the business.

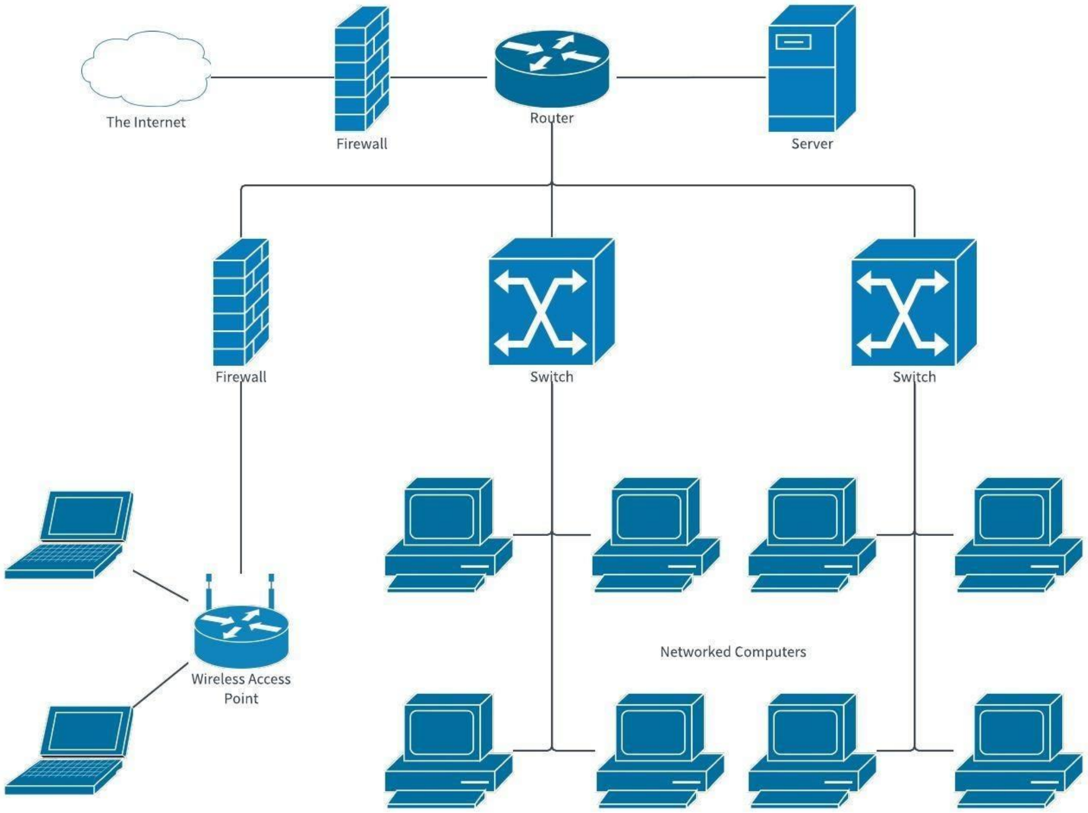
- Payment gateway: This is the software that enables secure online payment processing, such as credit card transactions.

- SSL certificate: This is a digital certificate that provides encryption for data sent between the web server and the customer's browser, ensuring that sensitive information is not intercepted by unauthorized parties.

- Database server: This is the computer that stores and manages the data related to the e-commerce website, including customer information, product details, and transaction records.

- Backup and recovery systems: These are essential components that help ensure that data is not lost in the event of a disaster, such as a system failure or natural disaster.

- Security systems: These include firewalls, intrusion detection and prevention systems, and antivirus software, all of which work together to protect the network from external and internal threats.



Architecture:

The architecture of a small business network design with a secure e-commerce server typically includes multiple layers of security and redundancy to ensure that the system is reliable and protected against various types of cyber-attacks. Here is a general overview of the architecture:

- Internet connection: The first layer of the architecture is the internet connection, which provides the gateway for the e-commerce server to communicate with the outside world. This connection should be secured using a firewall to block unauthorized access and protect against DDoS attacks.
- DMZ (demilitarized zone): The DMZ is a separate network segment that is isolated from the internal network and provides an additional layer of security for the e-commerce server. The DMZ typically contains the web server, payment gateway, and other external-facing components that need to be accessible from the internet. The DMZ is protected by a second firewall, which only allows traffic from the internet to reach specific ports and services.
- Internal network: The internal network is where the database server and other internal systems are located. Access to the internal network is restricted and only allowed through a VPN (virtual private network) connection or a secure login mechanism.
- Redundancy: Redundancy is important to ensure that the e-commerce server is always available, even in the event of hardware failure or other disruptions. Redundancy can be achieved by using multiple servers in a load-balanced configuration, as well as regular backups and disaster recovery plans.

- Security: Security is critical for an e-commerce server, which is why multiple layers of security are implemented in the architecture. In addition to firewalls and VPNs, other security measures include intrusion detection and prevention systems, antivirus software, and regular security audits and updates.
- Monitoring and logging: Monitoring and logging are essential for detecting and responding to security incidents and other issues. This includes monitoring network traffic, server logs, and other system activity to identify potential threats and vulnerabilities.

Disadvantages:

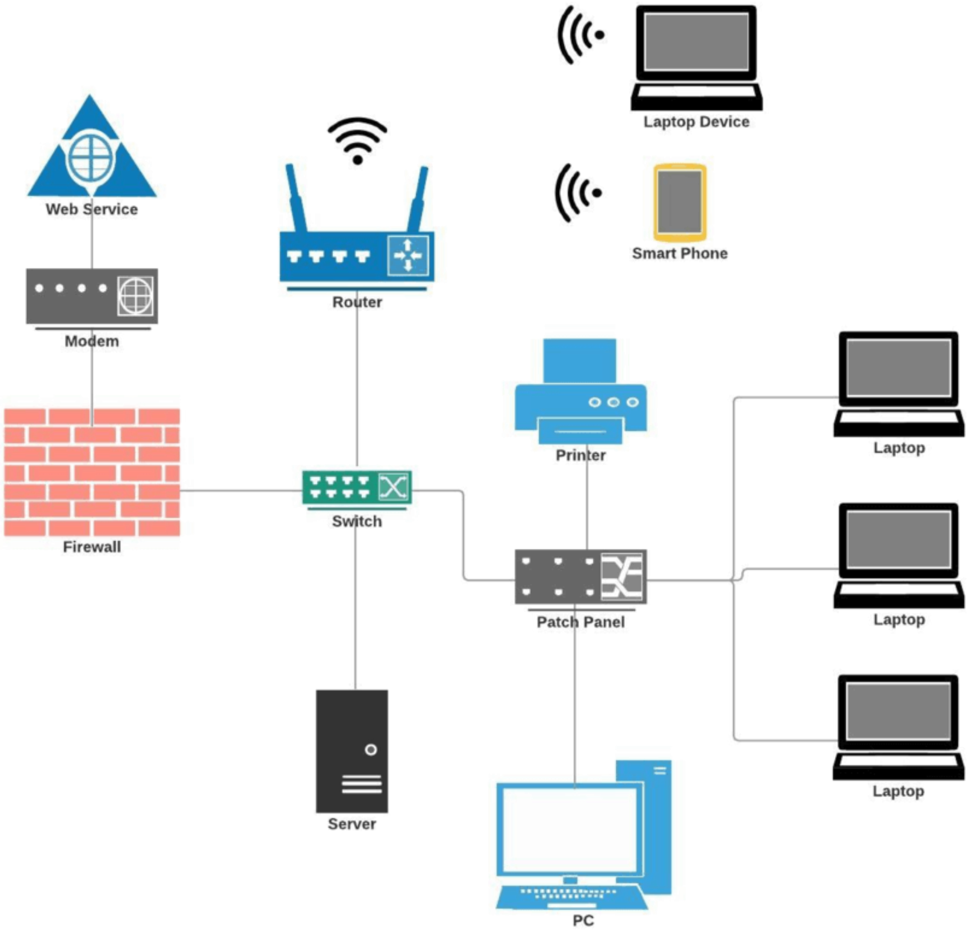
While there are many advantages to having a small business network design with a secure e-commerce server, there are also several potential disadvantages to consider:

- Cost: Implementing a secure e-commerce server can be costly, as it requires specialized hardware and software, as well as ongoing maintenance and security updates.
- Complexity: A small business network design with a secure e-commerce server can be complex, and it requires expertise in areas such as network architecture, web development, and cybersecurity.
- Downtime: Any network system can experience downtime, which can result in lost revenue and customer dissatisfaction. With an e-commerce server, downtime can be particularly damaging, as it can disrupt online transactions and damage the reputation of the business.
- Compliance: Depending on the industry and location, there may be specific regulations and compliance requirements that must be followed when implementing an e-commerce server. Failure to comply with these regulations can result in legal and financial penalties.

- Maintenance and Updates: E-commerce servers require regular maintenance and updates to ensure they remain secure and reliable. This can be time-consuming and require dedicated resour

Objective:

The main objective is to create a network in a simulator for a small business organization. The organization hosts an e-commerce application on a server which is accessible to internet users using https and with a public IP address securely.



Literature Survey:

- "Design and Implementation of E-commerce Website for Small Business" by R. K. Singh, et al. This research article provides an overview of the design and implementation of an e-commerce website for small businesses. The article covers topics such as website design, database design, and security considerations.

- "E-commerce Security: A Small Business Perspective" by E. M. Reimer and J. P. Muraski. This paper discusses the security challenges faced by small businesses when implementing e-commerce solutions. The authors provide recommendations for securing e-commerce systems and outline the importance of risk management and compliance.

- "Building Secure E-commerce Applications and Web Services" by S. Banerjee. This book provides an in-depth guide to building secure e-commerce applications and web services. The book covers topics such as web application security, authentication and authorization, and secure communication protocols.

- "Small Business Network Design" by M. L. Bannister. This book provides an overview of small business network design, including hardware and software considerations, network topology, and security considerations. The book also covers topics such as remote access and disaster recovery planning.

- "Security of E-commerce Systems" by P. O. Okewale and C. S. Adeyemo. This research article discusses the security issues that arise in e-commerce systems, including threats such as hacking, phishing, and identity theft. The authors provide recommendations for securing e-commerce systems and outline the importance of user education and awareness.

Requirements:

- Software: We use Cisco Packet Tracer in this project for better services, considering best security features. It provides the hardware and software services which can help us to mitigate any network related problem in future.
- Personal Computer (P.C): A personal computer can be defined as an end-point of connection which will connect with the computer network.
- Switches: A network switch (also called switching hub, bridging hub, and by the IEEE MAC bridge) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.
- Router: A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks

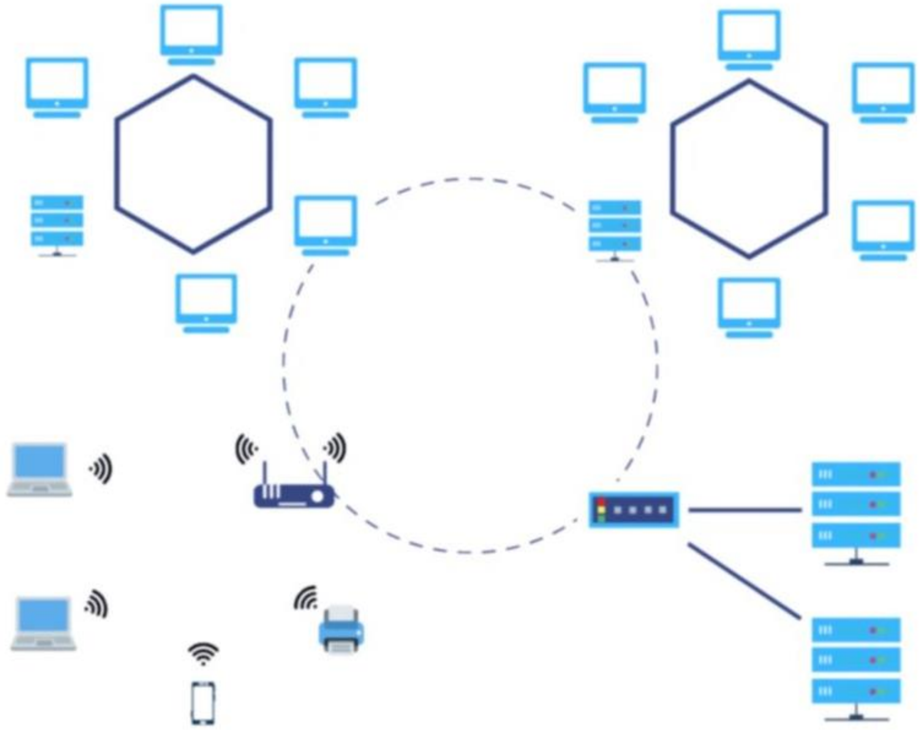
that constitute an internetwork (e.g. the Internet) until it reaches its destination node. A router is connected to two or more data lines from different IP networks. When a data packet comes in on one of the lines, the router reads the network address information in the packet header to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.

- Firewall: Firewall is a network security system that monitors and controls incoming and outgoing network traffics based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the internet.
- Server: In our project, we provide HTTPS Protocol in our server to enhance security. HTTPS protocol to transfer encrypted data/data’s over secure connection so HTTPS does encryption of data between a client and server, which protects against eavesdropping, forging of information and tampering of data.

Modules:

Our project deals with Small Business Network Design with Secure E-commerce server where it has the following three departments

- Internet users
- Security against malicious user
- Administration control



Modules description:

- Internet Users: Consists of people (Max 100 users) who wants to buy product/products from an e-commerce platform. Made it user friendly. Internet Service Provider: It consists of all internet services provider companies that provide a medium for passing the internet user and E-commerce Server respectively with having a specific and secure medium.
- Securities against malicious user: Duals protection (https & firewall) use for securities purpose with the information transfer between the other authorities and will be safe and secure for administrative computing.
- Administration Control: Administration Control maintains the origin design, update securities and privacy of the small business network. It also compliance regulatory requirements i.e. IP address, Network Address Translation (NAT), Access Control List (ACL), etc. A network has to be designed for a small business organization which has 100 users. The organization hosts an e-commerce application on a server which is accessible to internet users using https and with a public IP address.

Hardware List:

Devices	Required No’s
PCs	6
Router	1
Server	1
ASA	1
Copper Cross Over	2
Copper Straight-Through	6
Console	1

E-Commerce Security Standards:

Businesses, small and large, are required to comply with certain laws and regulations related to their activities. The concern for security has led to the development of standards and regulations to safeguard valuable data.

ISO 17799 provides recommendations for the following:

• Asset Classification and Control- All information assets should be accounted for and have security classifications to indicate the need and priorities for protection.

• Personnel security- Personnel should be provided appropriate security education and be aware of the incident reporting procedures.

• Physical and Environmental Security

• Network Security

• Access Control

Security Policies

Any organization concerned with protecting its electronic commerce assets should have a security policy in place. The security policies should describe which assets to protect and why, who is responsible for their protection, and what is acceptable and what is not. Security policies act as a guide for employees so they know what to do before, during and after an incident. The employees should all be aware of the policies, and tests can be conducted to ensure their competency. Tests can be in a variety of forms, such as written, oral and scenario-based tests. The tests should be designed so that employees are comfortable with the information in the policies and are comfortable responding to a variety of situations.

Physical Security

Physical security should be the first type of security that is implemented. It doesn’t make sense to secure your computer and leave your place unsecure; that is almost the same as locking the doors to your home but leaving the windows open. Physical security can even be in the form of video monitoring systems and access control devices. While there is no way to be completely secure, it is best to limit the chances of being a victim.

Access Control

Controlling access to a facility or regions in the facility is an important part of security. Security guards should be used for roving patrols and ID verification of employees. The problem with security guards is that they are human and social engineering can be used to manipulate them. Because of the social engineering concerns, locks, biometrics scanners, and passwords should also be considered for access control.

Monitoring

Monitoring is very important because a hacker could sneak in without a company knowing and cause a lot of damage. The facility and the network need to be monitored to prevent a hacker from penetrating defences and causing irreversible damage. With constant monitoring, security will be able to detect an attack and stop it before damage occurs. It is better to take measures to prevent something from happening than to try to repair the damage later. Some things may be damaged beyond repair and important information could be lost forever.

Authentication

Different methods of verification are used by different agencies to prevent unauthorized users from accessing their facilities, systems, and services.

Biometrics

Biometrics uses a person’s body for access verification. Retinal scans, finger and palm print readers, and other body scanners are used for access control to verify a person’s identity. Biometrics is good because it uses parts of the body that are unique to that individual. The problem with biometrics comes when a person damages their part of the body that is used for verification. If a person damages the body part used for verification, it will require extra work and the administrator will have to use a different means to allow that person access.

Usernames and Passwords

Usernames and passwords are user chosen credentials, which usually have certain requirements that are set by administrators. Requirements have to be set because people will use passwords that are common and hackers can break them. “The most secure passwords are at least 8 characters long with a mixture of upper- and lower-case letters and symbols and numbers. The problem with passwords and usernames is that people either forget them or they write them down and put them in a place where people can find them.

Smartcards

Smart Cards are used in many facilities to control access to a certain area, system, or service. Smartcards allow a person access without having to remember a password. The problem with many smartcards is that people lose them and other people might be able to use them.

Wireless Security

The days of connecting computers with wires are gone; now businesses use wireless connections to send, receive and access information. Sending and receiving information wirelessly makes it susceptible to being apprehended. Systems can send and receive information via a wireless router that is connected to a modem which is connected to the Internet. The computers send out packets to the wireless router, which then transfers that to the modem and through the Internet.

Cryptography

Cryptography is used to turn plaintext into an algorithm known as ciphertext, which is a complex mathematical sequence unreadable to anybody without the code to decipher it. Once data is encrypted into ciphertext, it is given a password and that password is needed to decrypt the data and turn it back into plaintext. That data can be sent to another person as long as that person has the password to decrypt the information. The type of algorithm determines the strength of the encryption and can make it more or less difficult to decrypt without the proper key. Cryptography is also used to create signatures for documents, which help to determine originality of that document.

Hashing

Hashing is a way of creating a unique signature for a document to prove that the document is the original document. Hashing is used to compare to the document to ensure it is the original. The most secure type of hash is the Secure Hash Algorithm (SHA), which uses 160 bit encryption.

Computer Intrusion Detection and Prevention Systems

Computer Intrusion Detection and Prevention Systems are similar to having amotion detector on the building and locks on the doors and windows. The Computer Intrusion Detection (IDS) System, similar to the motion detector, is meant to detect potential attackers and alert someone to take action. The Intrusion Prevention System (IPS), similar to the locks on the doors and windows, is meant to keep the attacker out. The names of the two systems sums up exactly what they are meant for. To have a good security program, you need both protection systems in place; one for detection and the other for prevention of malicious activity. Many systems these days incorporate both detection and prevention into one system and are known as Intrusion Detection and Prevention Systems (IDPS).

Intrusion Detection Systems

IDS monitors a network for possible malicious activity and then reports that activity to the

administrator so he or she can make a decision on what to do with that threat. There are many different types of IDS's, which use different protocols for detection of threats such as network based, wireless, behaviour analysis, and host-based detection systems. e-commerce systems should deploy both network and host-based IDS, however the cost might be too much for some small businesses.

Host-Based IDS

The functionality of host-based IDS's are similar to a virus scanner tool. The software is automated and runs in the background of the host system to detect any suspicious activities. It can be configured to take specific actions when an issue is detected. For example, it can be configured to automatically quarantine the suspicious activity or simply notify the administrator of the issue.

Network-Based IDS

Network-Based IDS’s examine the type and content of network packets. Network IDS’s are less expensive than host-based IDS’s, but it cannot monitor activities on individual host systems. It can protect the network as a whole but cannot protect individual systems. When choosing the IDS, it needs to be compatible with the firewall that is being used. The network-based IDS should be deployed between the incoming connections and the firewall. It should also be installed under two network interfaces, one for analysing and one for reporting information to the IDS console.

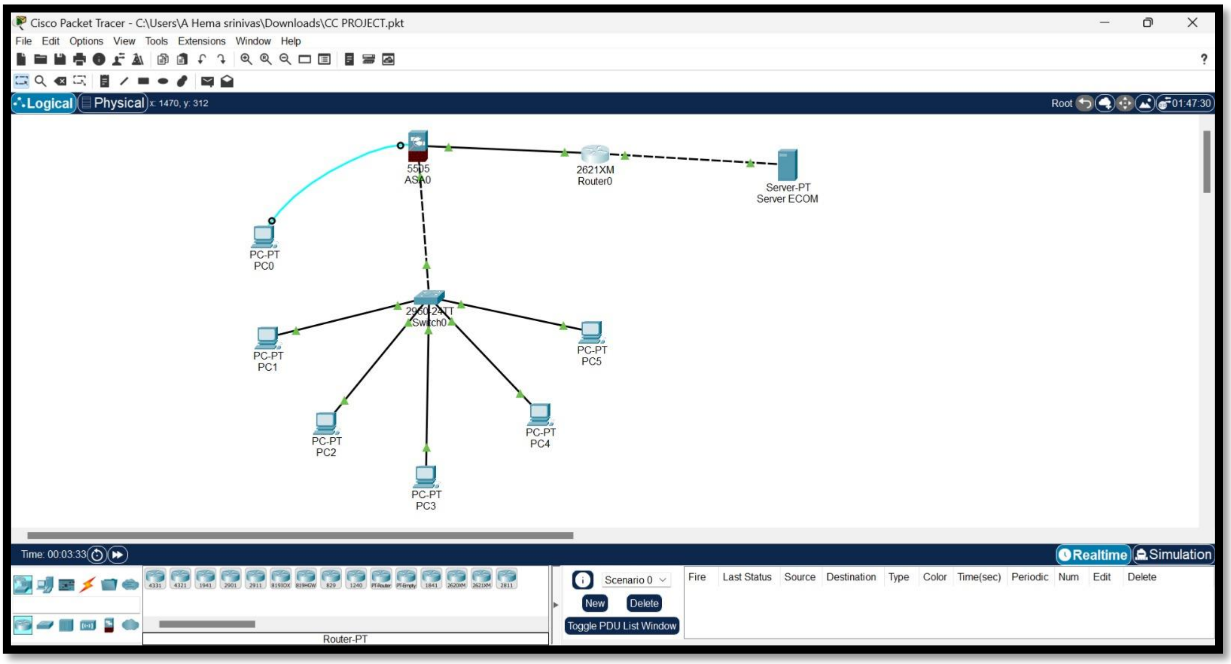
Intrusion Prevention System

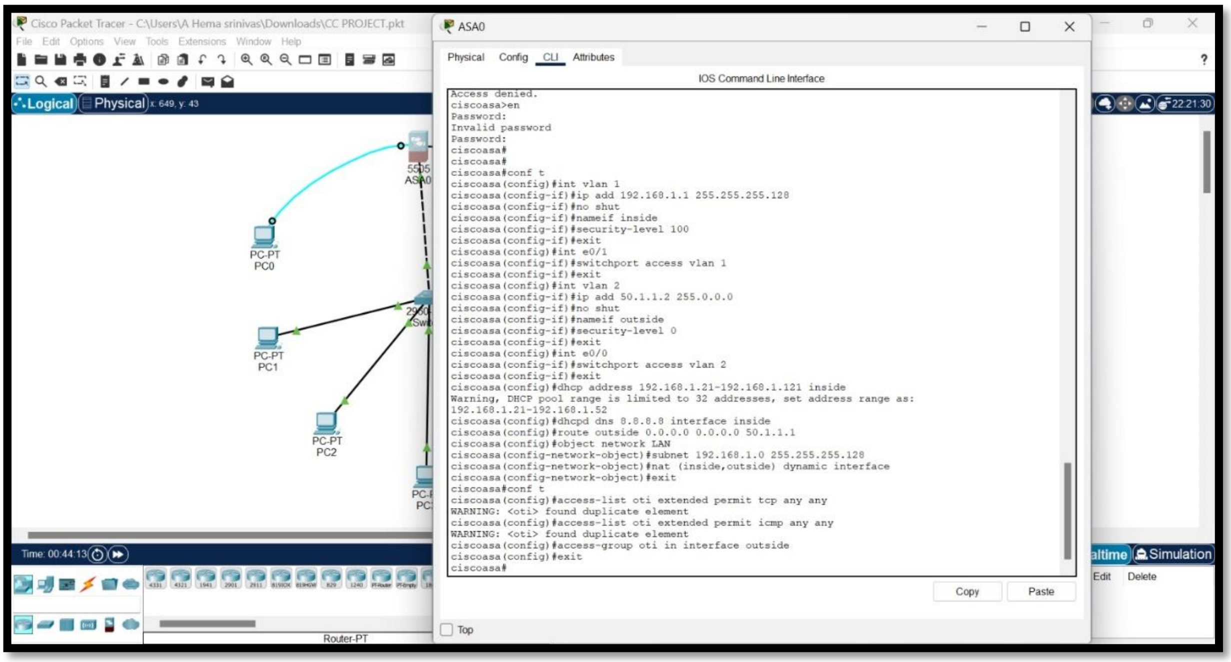
IPS’s use a certain protocol of identifying threats and preventing them from accessing a network so they do not have a chance to harm the system. IPS’s monitor the network traffic for malicious activity, log the activity, attempt to prevent it from accessing the network, and then report the activity to the administrator so he or she can follow-up with an action. Just like the IDS, the IPS may detect activity that is not malicious and the administrator will have to decide what to do with it.

Operating System Hardening

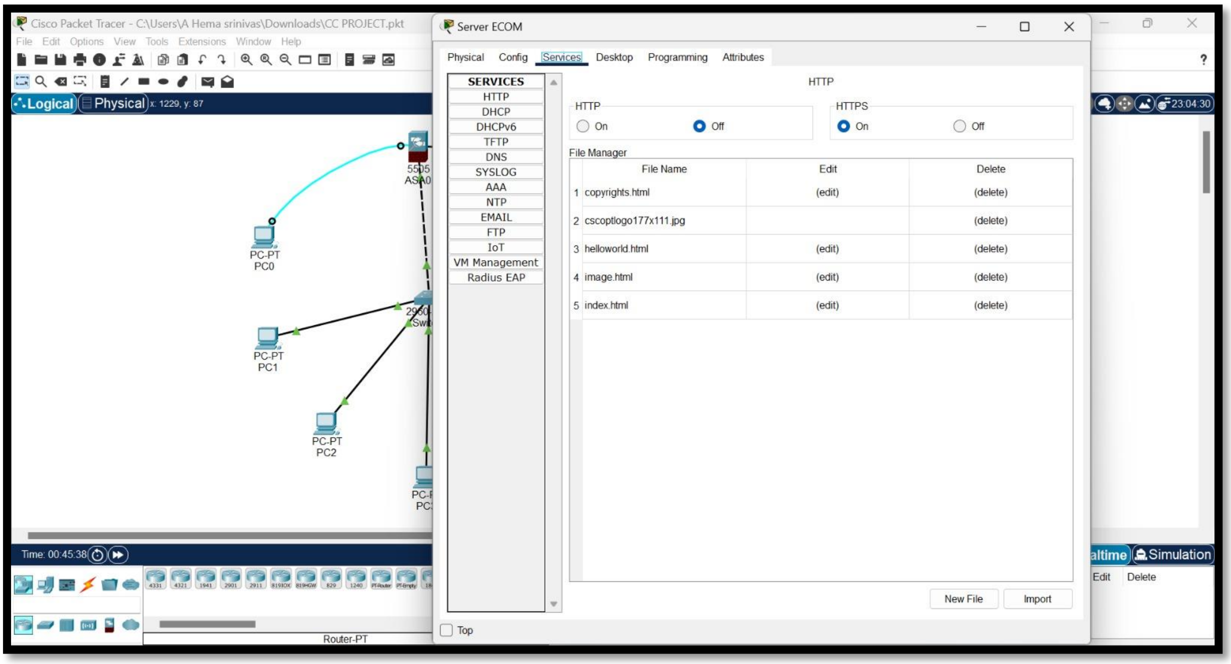
In e-commerce systems, it is important to reduce the attack possibilities by reducing or eliminating as many vulnerabilities as possible. This is accomplished by incorporating IDS's, installing anti-virus systems, removing all unnecessary programs, closing all ports and configuring it to protect against unauthorized access. "In many instances, an operating system provides a gateway into a computer system because of the large number of open ports and services running. Many types of security software can be configured to detect and automatically handle suspected incidents. It is important to look for software that has low false-positives because it could potentially hurt business if it is blocking transactions from occurring instead of blocking attempted attacks. Also, it is important to find the software that has a good team and offers continuous updates. Threats are constantly evolving and it is important for software companies to stay up-to-date with the latest threats to their software. It will be important to continually check for updates and patches so vulnerabilities in the software are fixed before an attack occurs.

OUTPUT:





```
Access denied.
ciscoasa>en
Password:
Invalid password
Password:
ciscoasa#
ciscoasa#
ciscoasa#conf t
ciscoasa(config)#int vlan 1
ciscoasa(config-if)#ip add 192.168.1.1 255.255.255.128
ciscoasa(config-if)#no shut
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#exit
ciscoasa(config)#int e0/1
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#exit
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip add 50.1.1.2 255.0.0.0
ciscoasa(config-if)#no shut
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#exit
ciscoasa(config)#int e0/0
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#exit
ciscoasa(config)#dhcp address 192.168.1.21-192.168.1.121 inside
Warning, DHCP pool range is limited to 32 addresses, set address range as:
192.168.1.21-192.168.1.52
ciscoasa(config)#dhcpd dns 8.8.8.8 interface inside
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 50.1.1.1
ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.128
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#exit
ciscoasa#conf t
ciscoasa(config)#access-list oti extended permit tcp any any
WARNING: <oti> found duplicate element
ciscoasa(config)#access-list oti extended permit icmp any any
WARNING: <oti> found duplicate element
ciscoasa(config)#access-group oti in interface outside
ciscoasa(config)#exit
ciscoasa#
```



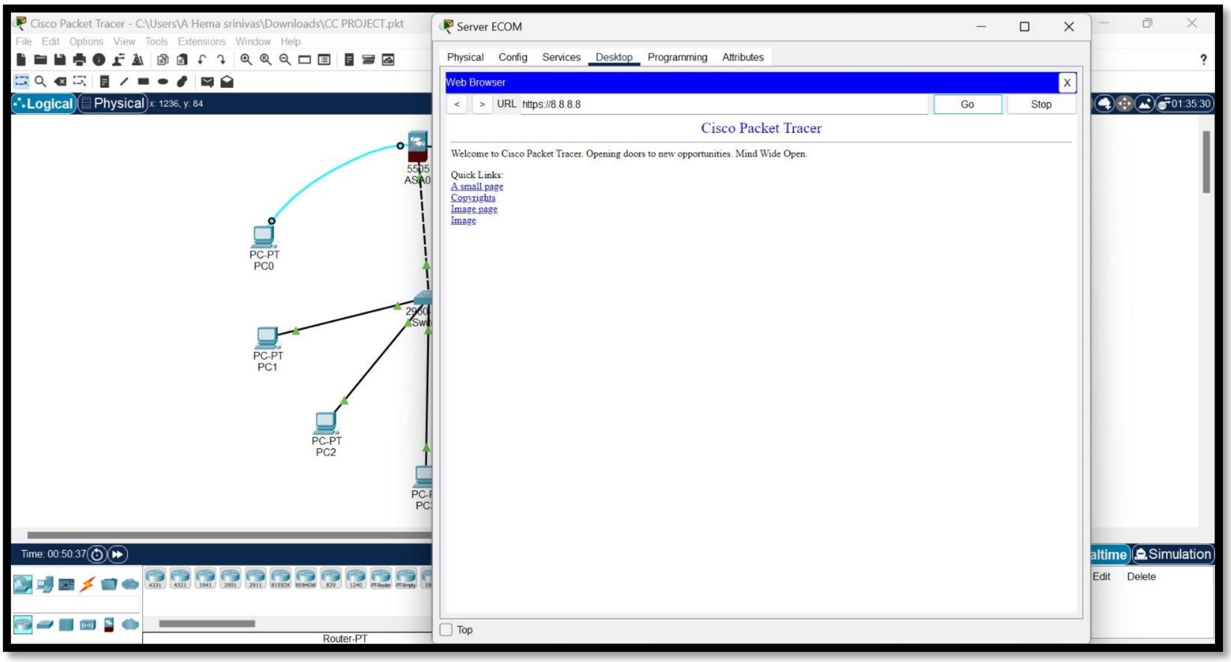
HTTP

HTTP: ○ On ● Off

HTTPS: ● On ○ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

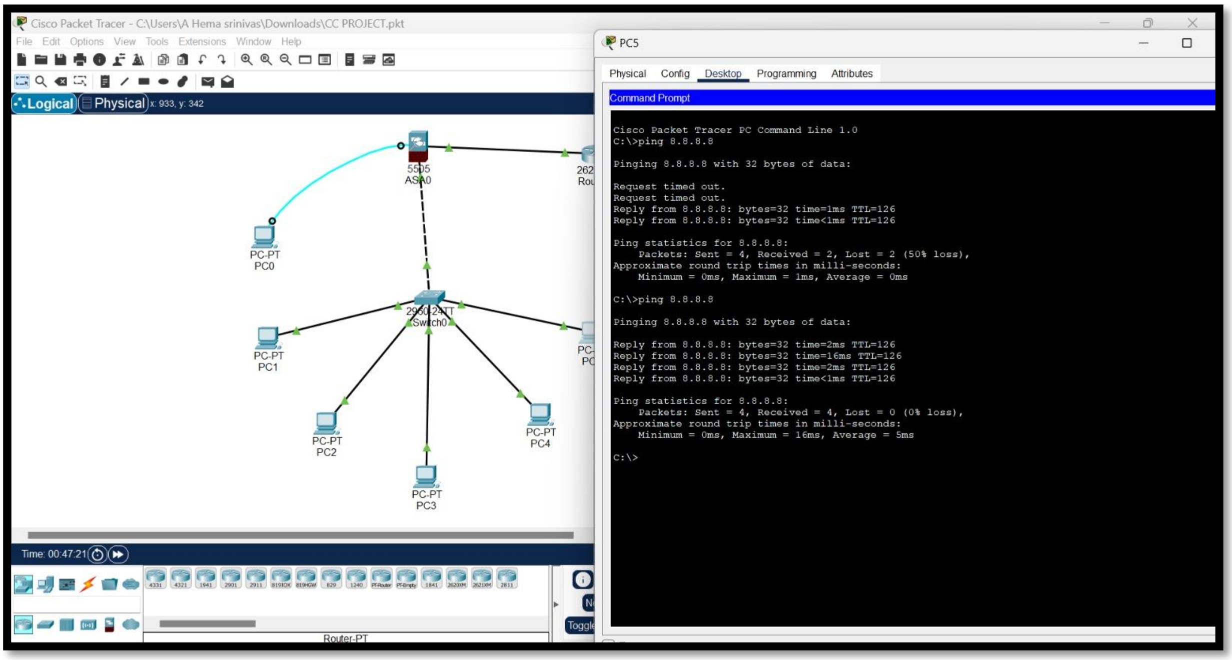


URL https://8.8.8.8

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=2ms TTL=126
Reply from 8.8.8.8: bytes=32 time=16ms TTL=126
Reply from 8.8.8.8: bytes=32 time=2ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 5ms

C:\>
```

CLI :

Router Configuration: -

For IP ADDRESS

```
Router> en

Router> conf t

Router(config)# int f0/0

Router(config-if)# ip add 50.1.1.1 255.0.0.0 R outer(config-if)# no shut

Router(config)# int f0/1

Router(config-if)# ip add 8.8.8.1 255.0.0.0

Router(config-if)# no shut

Router(config-if)# exit
```

For Network Address Translation (NAT)

```
Router(config)# router rip

Router(config-router)# network 8.0.0.0

Router(config-router)# network 50.0.0.0

Router(config-router)#exit

Router# conf t

Router(config-if)# ip route 0.0.0.0 0.0.0.0 192.168.1.1

Router(config-if)# ip route 0.0.0.0 0.0.0.0 8.8.8.8
```

Firewall Configuration:

For IP ADDRESS

```
Ciscoasa> en

Ciscoasa# conf t

Ciscoasa(config)# int vlan 1

Ciscoasa(config-if)# ip add 192.168.1.1 255.255.255.128
Ciscoasa(config-if)# no shut
Ciscoasa(config-if)# nameif inside
Ciscoasa(config-if)# security-level 100
Ciscoasa(config-if)# exit
Ciscoasa(config)# int e0/1
Ciscoasa(config-if)# switchport access vlan 1
Ciscoasa(config-if)#exit
Ciscoasa(config)# int vlan 2
Ciscoasa(config-if)# ip add 50.1.1.2 255.0.0.0 Ciscoasa(config-if)# no shut
Ciscoasa(config-if)# nameif outside
Ciscoasa(config-if)# security-level 0
Ciscoasa(config-if)# exit
Ciscoasa(config)# int e0/0
Ciscoasa(config-if)# switchport access vlan 2
Ciscoasa(config-if)#exit
Ciscoasa(config)# dhcpd address 192.168.1.21-192.168.1.121 inside
Ciscoasa(config)# dhcpd dns 8.8.8.8 interface inside
Ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 50.1.1.1
```

For Network Address Translation (NAT)

```
Ciscoasa(config)#object network LAN
Ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.128
Ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
Ciscoasa(config-network-object)# exit
```

For Access Control List (ACL)

```
Ciscoasa# conf t
Ciscoasa(config)# access-list oti extended permit tcp any any
Ciscoasa(config)# access-list oti extended permit icmp any any
Ciscoasa(config)# access-group oti in interface outside
Ciscoasa(config)# exit
```

Server E-Com: -

1. Click E-Com Servet. Then go to services.
2. Then on left hand side, go to HTTP.
3. Then Turn OFF the HTTP and Turn ON the HTTPS.
4. Make the changes According and save it.

Inference:

E-commerce is an effective way to do business. It allows businesses to provide products and services to a wider population than they could with traditional brick and mortar operations. However, e-commerce also comes with a wide variety of risks that need to be mitigated to

operate securely. Small businesses provide an easy target for attackers because they typically have limited funding and do not have dedicated network professionals to monitor and protect their network. Hackers have a wide variety of tools that allow them to attack networks even with little technical knowledge. Hackers use a system along with their tools to attack systems. They first need to gather as much information as possible about the target system, scan for open ports, scan for vulnerabilities and then conduct their attack. Along with technical attacks, some attackers might try physical attacks through social engineering and gain access to the business servers by pretending to be someone they are not. Small businesses need to take as many precautions as possible to protect their systems, even if it means spending extra money to do so. There is really no way of completely securing a network, but there are ways to minimize the chances of becoming a victim. Limiting the chances of becoming a victim is better than trying to repair the damages after an attack, which may not be repairable. Attacks come in many forms, so it is imperative to ensure that as many security measures are put in place as possible. The implementation of various security measures is important for the protection of family, business continuity and national security. With the possible outcomes of an attack on a network, businesses should take network security very seriously and properly protect their systems

References:

[1] Brenton, C. (2003). Mastering Network Security. 2nd ed. Alameda,CA: Sybex

[2] Center of Excellence Defence Against Terrorism (2008). Responses to Cyber Terrorism. Amsterdam,NLD: IOS Press.

[3] Ciampa, M. (2009). CompTIA Security+ 2008 In Depth. Boston, MA: Course Technology.

[4] Dent, A., Mitchell, C. (2005). User's Guide to Cryptography and Standards. Norwood,

MA: ArtechHouse, Incorporated.

[5] Department of Homeland Security (2003). The National Strategy to Secure Cyberspace. RetrievedMarch 01, 2011 from:

http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pf

[6] DevCenter (n.d.). INFO: Understanding PCI Compliance.

Retrieved from:http://dev.ektron.com/kb_article.aspx?id=26304