Computer Communications

Project

Small Business Network Design with Secure E-commerce Server

Submitted By

R.SHIVA KUMAR(RA2011031010017)

S. SANCHAY KUMAR(RA2011031010049)

A.VISHAL ARAVINTH(RA2011031010013)

Project Title – Small Business Network Design with Secure E-commerce server

E-Commerce:

An eCommerce website is an online destination where buyers shop for goods and sellers offer products and services. It's the hub of information about a company and what they sell. On an eCommerce website, you'll find product listings, eCommerce blog content, company history, and contact information.

You can sell just about anything through an eCommerce site. Examples include recreational equipment, car and motorcycle parts, household goods, clothing and jewelry, and food and drinks. If you need help coming up with additional ideas, consider these wholesale items to sell or high demand products.

The data generated by an eCommerce website isn't only useful for sellers and buyers. It's also used by shipping and handling providers, 3PL companies, marketers, and warehouse inventory management software.

eCommerce websites can be created by a specialized agency, web developer, or your own skills. The size and needs of your site play a major part in which choice is best.

If you're just starting an eCommerce business and only sell a few products, you can get an excellent website created for a few hundred dollars or less. If you sell thousands of products or are revamping your entire brand, working with a dedicated developer is a smart call.

There's also the option of using pre-made website builders. Looking for a dropshipping website builder, or subscription

website builder if you want to sell a subscription box, will save you time. Services that offer this, like WordPress, Shopify, and Wix, make it easy to customize a website framework. You can also review some of the best dropshipping websites, and best eCommerce websites to get a feel for what customers expect.

E-commerce involves the process of buying, selling, and exchanging of products, services, and information via computer networks, primarily through an Internet. But 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 organization 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. The objective of this project is to identify obstacles that facing the implementation of ecommerce system and providing security solutions to protect sensitive information.

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 Project will discuss how attacks are carried out and how a small business can effectively secure their networks with minimum cost. In the project, we have tried to make the design of project which is user friendly and secure for customer. They can easily

search and buy any product/products any time (24 X 7) without facing any malicious attack through an Internet. We introduced protection by using firewall between customer-server and https protocol.

Project Scope:

To design a network 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 securely.

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.

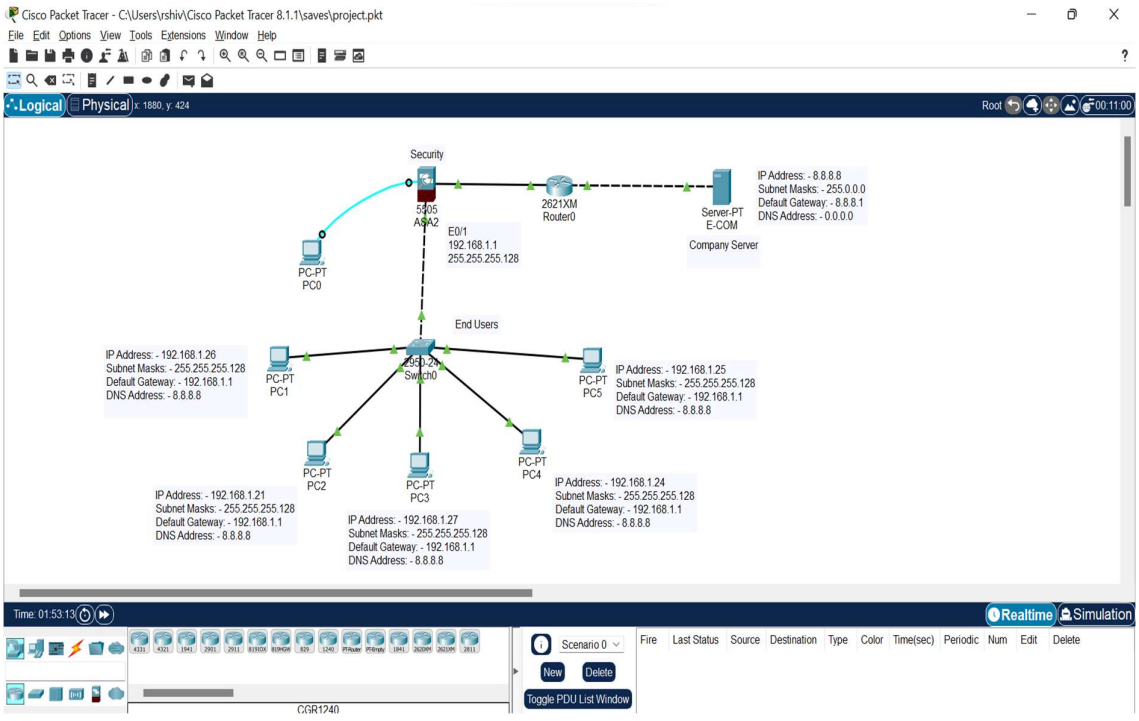
Requirements Analysis:

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

- **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.

Network Diagram:



TCP/IP Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway	DNS Address
PC0	Fa0/0	-	-	-	-
PC1	Fa0/0	192.168.1.26	255.255.255.128	192.168.1.1	8.8.8.8
PC2	Fa0/0	192.168.1.21	255.255.255.128	192.168.1.1	8.8.8.8
PC3	Fa0/0	192.168.1.27	255.255.255.128	192.168.1.1	8.8.8.8
PC4	Fa0/0	192.168.1.24	255.255.255.128	192.168.1.1	8.8.8.8
PC5	Fa0/0	192.168.1.25	255.255.255.128	192.168.1.1	8.8.8.8
Server	Fa0/0	8.8.8.8	255.0.0.0	8.8.8.1	0.0.0.0
Firewall	E0/0	50.1.1.2	255.0.0.0	-	-
Firewall	E0/1	192.168.1.1	255.255.255.128	-	-
Router	F0/0	8.8.8.1	255.0.0.0	-	-
Router	F0/1	50.1.1.1	255.0.0.0	-	-

E-commerce server: -

1.Server: -

Property	Value
Name	E-com
I.P Address	8.8.8.8
Subnet	255.0.0.0
Default Gateway	8.8.8.1
DNS Address	0.0.0.0

2.Router:-

Property	Value
Name	Router
Interface	F0/1
I.P Address	8.8.8.1
Subnet	255.0.0.0
Port Status	ON
Interface	F0/0
I.P Address	50.1.1.1
Subnet	255.0.0.0
Port Status	ON

Internet Users: -

PCs with switch 0: -

1.

Property	Value
Name	PC1
I.P Address	192.168.1.26
Subnet	255.255.255.255.128
Default Gateway	192.168.1.1
DNS Address	8.8.8.8

2.

Property	Value
Name	PC2
I.P Address	192.168.1.21
Subnet	255.255.255.128
Default Gateway	192.168.1.1
DNS Address	8.8.8.8

3.

Property	Value
Name	PC3
I.P Address	192.168.1.27
Subnet	255.255.255.128
Default Gateway	192.168.1.1
DNS Address	8.8.8.8

4.

Property	Value
Name	PC4
I.P Address	192.168.1.24
Subnet	255.255.255.128
Default Gateway	192.168.1.1
DNS Address	8.8.8.8

5.

Property	Value
Name	PC5
I.P Address	192.168.1.25
Subnet	255.255.255.128
Default Gateway	192.168.1.1
DNS Address	8.8.8.8

Firewall:-

Property	Value
Name	ASA
Interface	E0/0
I.P Address	50.1.1.2
Subnet	255.0.0.0

Port Status	**ON**
Interface	**E0/1**
I.P Address	**192.168.1.1**
Subnet	**255.255.255.128**
Port Status	**ON**

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.

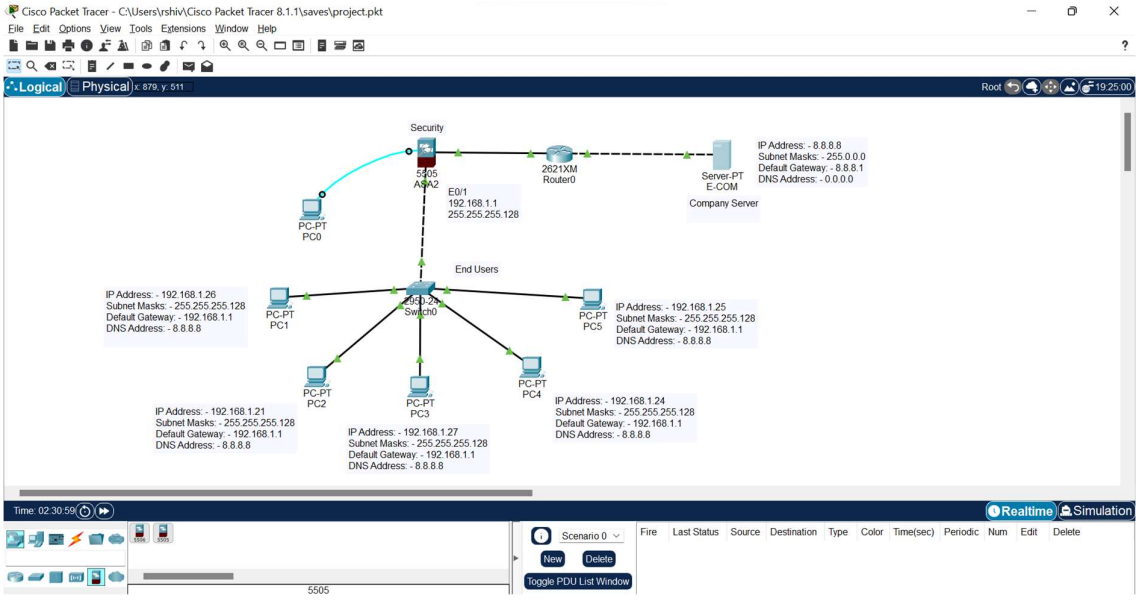
4. Make the changes According and save it.

Hardware List:

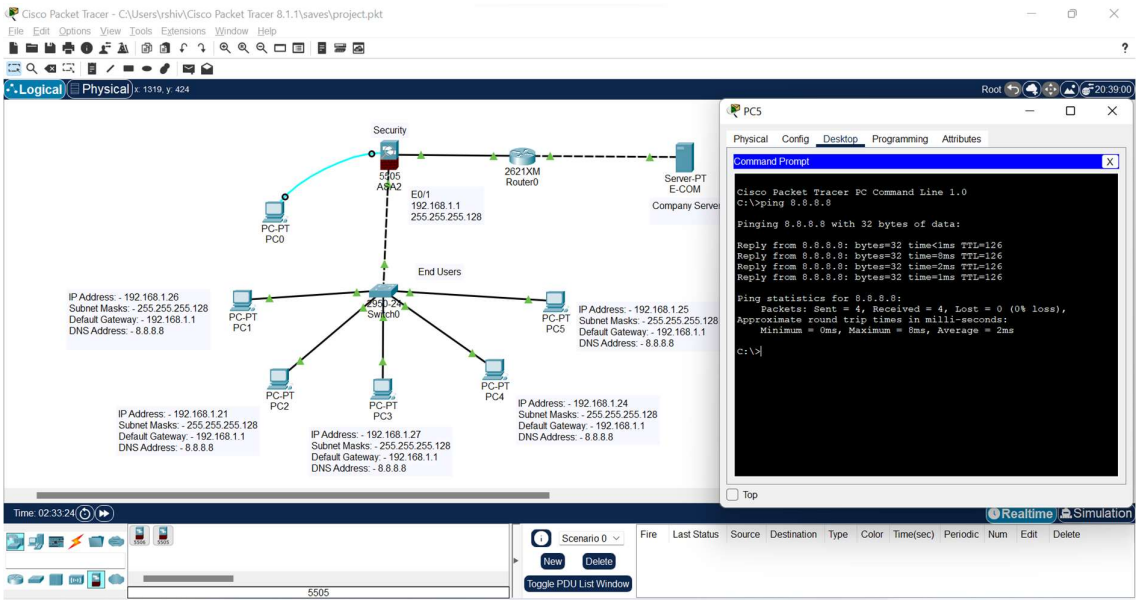
Devices	Required No's
PCs	**6**
Router	**1**
Server	**1**
ASA	**1**
Copper Cross Over	**2**
Copper Straight-Through	**6**
Console	**1**

Project Screenshots:

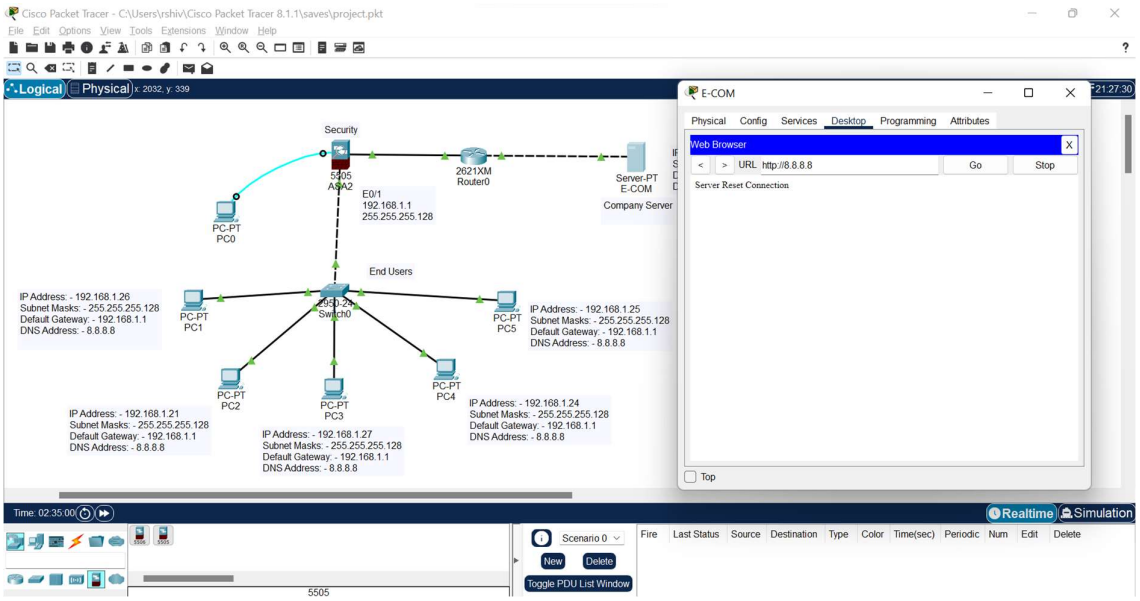
1. Small Business Network Design with Secure E-commerce server



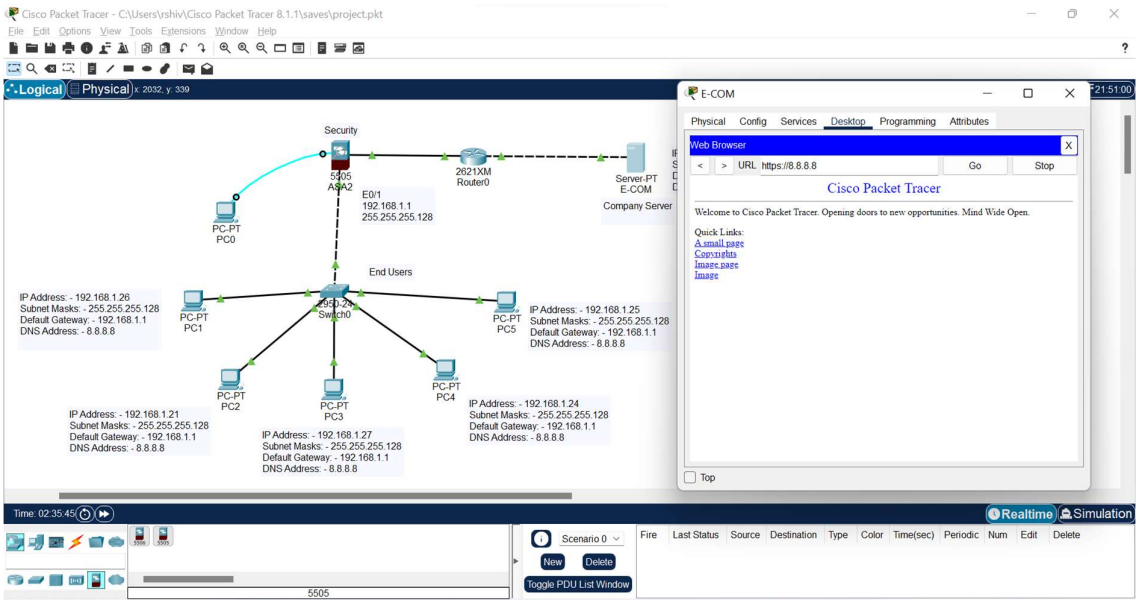
2.Ping to Server



3.Website access without HTTPS



4.Website access with HTTPS:



Packet Tracer File:-

SmallBusinessNetwo
rkDesignwith.pkt

References:

1. https://networklessons.com/cisco/asa-firewall/cisco-asa-security-levels

2. https://networklessons.com/cisco/asa-firewall/cisco-asa-access-list

3. https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generationfirewalls/115904-asa-config-dmz-00.html

4. https://www.youtube.com/watch?v=jOYvI6aBVE8

5. https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-defaultrouting-in-cisco-routers.html

5. https://www.computernetworkingnotes.com/ccna-study-guide/static-routingconfiguration-guide-with-examples.html