SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be **University** *u/s 3 of UGC Act, 1956*

Small Business Network Design with Secure E-commerce Server

A PROJECT REPORT

Submitted by

Jay Agrawal

ABSTRACT

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 dual protection by using firewall between customer-server and https protocol.

OBJECTIVE

To design a proposal for setting up a network in an E-commerce mainly having the three major departments i.e. An E-commerce security, small business organization & service providers and 100 internet users.

E-commerce (electronic commerce) is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. These business transactions occur either as business-to-business (B2B), business-to-consumer (B2C), consumerto-consumer or consumer-to-business. The terms e-commerce and e-business are often used interchangeably. The term e-tail is also sometimes used in reference to the transactional processes for online shopping.

In the last decade, widespread use of e-commerce platforms such as Amazon and eBay have contributed to substantial growth in online retail. In 2007, e-commerce accounted for 5.1% of total retail sales; in 2019, e-commerce made up 16.0%. New studies projected that the worldwide retail eCommerce sales will reach a new high by 2021. Ecommerce businesses should anticipate a 265% growth rate, from $1.3 trillion in 2014 to $4.9 trillion in 2021. This shows a future of steady upward trend with no signs of decline. There are various types of e-commerce threats. The most common security threats are phishing attacks, money thefts, data misuse, hacking, credit card frauds, and unprotected services. Inaccurate management-One of the main reasons for ecommerce threats is poor management.

There are many types of network security solutions that you'll want to consider, including:

Access control: Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC).

Antivirus and antimalware software: "Malware," short for "malicious software," includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

Application security: Any software you use to run your business needs to be protected, whether your IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, that attackers can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes.

Firewalls: Firewalls put up a barrier between your trusted internal network and untrusted outside networks, such as the Internet. They use a set of defined rules to allow or block traffic. A firewall can be hardware, software, or both. Cisco offers unified threat management (UTM) devices and threat-focused next-generation firewalls (NGFW).

Network segmentation: Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. You can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.

Web security: A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

INTRODUCTION

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.

MODULES

Below, are the definitions of the individual modules used in the project-

A2Z Mart 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.

Also, HTTPS ensures data security over the internet mainly public network like Wi-Fi. By virtue, HTTPS encryptions is done bi-directionally, which means that the data is encrypted at both the client and server site. Only the client can decode the information that comes from the server.

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.

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.

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.

A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

ISP 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.

Personal Computer (P.C): A personal computer can be defined as an end-point of connection which will connect with the computer network.

MODULE DESCRIPTION

E-commerce server: -

1.Server: -

Property	Value
Name	A2Z Mart
IP 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	ISP Router
Port 1 Name	F0/1
IP Address	8.8.8.1
Subnet	255.0.0.0
Port Status	ON
Port 2 Name	F0/0
IP Address	50.1.1.1

Subnet	255.0.0.0
Port Status	ON

Internet Users: - PCs

with switch 0: -

1.

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

2.

Property	Value
Name	PC1
I.P.	192.168.1.22
Subnet	255.255.255.128
Default Gateway	192.168.1.1
DNS Address	8.8.8.8

3.

Property	Value
Name	PC3

I.P.	192.168.1.23
Subnet	255.255.255.128
Default Gateway	192.168.1.1
DNS Address	8.8.8.8

4.

Property	Value
Name	PC4
I.P.	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.	192.168.1.25
Subnet	255.255.255.128
Default Gateway	192.168.1.1

Firewall: -

Property	Value
Name	ASA

Port 1 Name	E0/0
IP Address	50.1.1.2
Subnet	255.0.0.0
Port Status	ON
Port 2 Name	E0/1
IP Address	192.168.1.1
Subnet	255.255.255.128
Port Status	ON

Configuration: -

Router: -

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
Router(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: -

For IP ADDRESS

```
Ciscoasa> en
Ciscoasa# conf t
Ciscoasa(config)# int vlan 1
Ciscoasa(config-if)# ip add 192.168.1.1 255.255.252.128
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
```

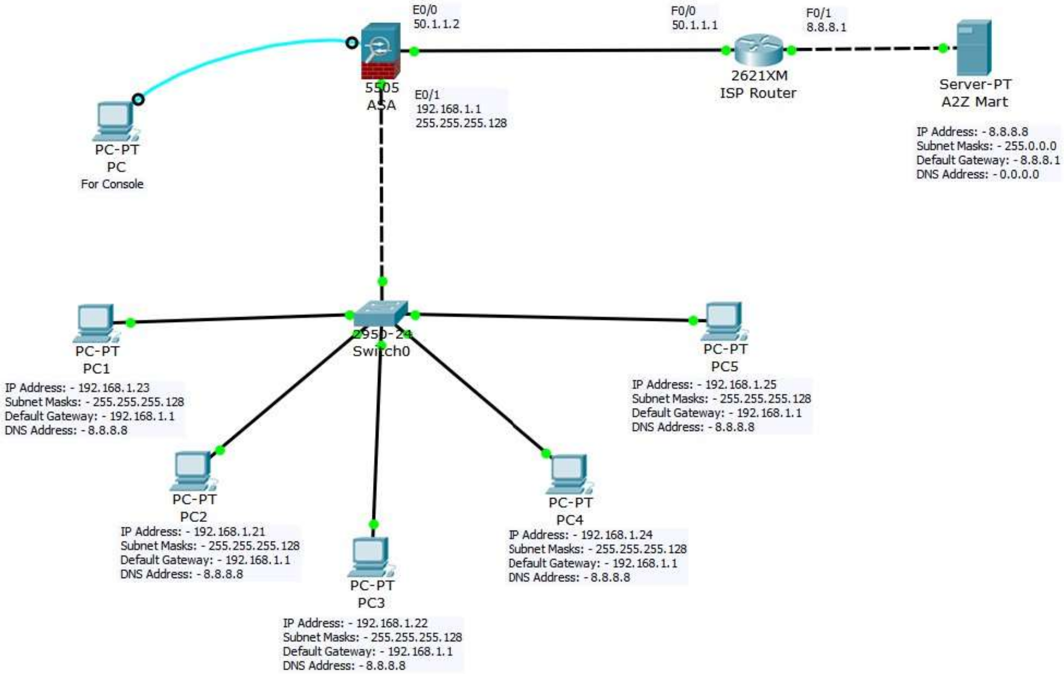
For Access Control List (ACL)

```
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
```

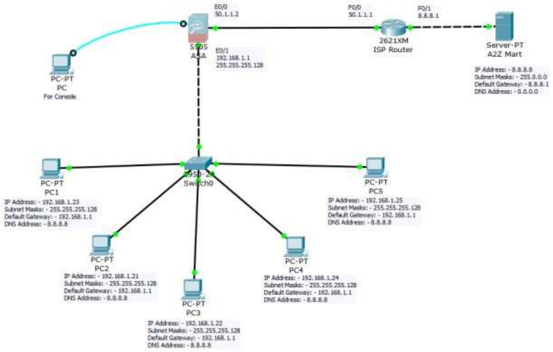
Server: -

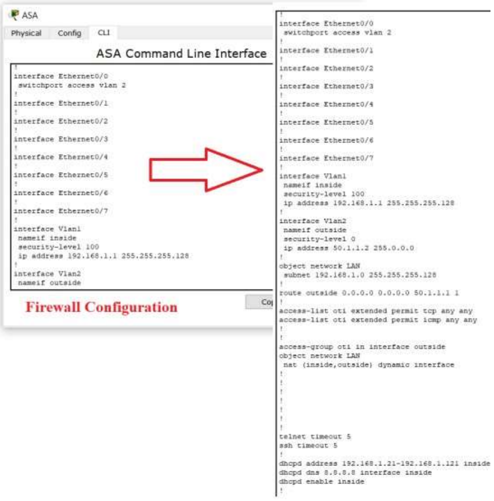
1. Click A2Z Mart. Then go to services.
2. Then on left hand side, go to HTTP.
3. Then Turn OFF the HTTP and Turn ON the HTTPS.
4. Make the changes According and save it.

PROJECT SNAPSHOT


E0/0
50.1.1.2
F0/0
50.1.1.1
F0/1
8.8.8.1
5505
ASA
E0/1
192.168.1.1
255.255.255.128
2621XM
ISP Router
Server-PT
A2Z Mart
IP Address: - 8.8.8.8
Subnet Masks: - 255.0.0.0
Default Gateway: - 8.8.8.1
DNS Address: - 0.0.0.0
PC-PT
PC
For Console
2950-24
Switch0
PC-PT
PC1
IP Address: - 192.168.1.23
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC5
IP Address: - 192.168.1.25
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC2
IP Address: - 192.168.1.21
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC4
IP Address: - 192.168.1.24
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC3
IP Address: - 192.168.1.22
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8

Small Business Network Design with Secure E-commerce Server Model



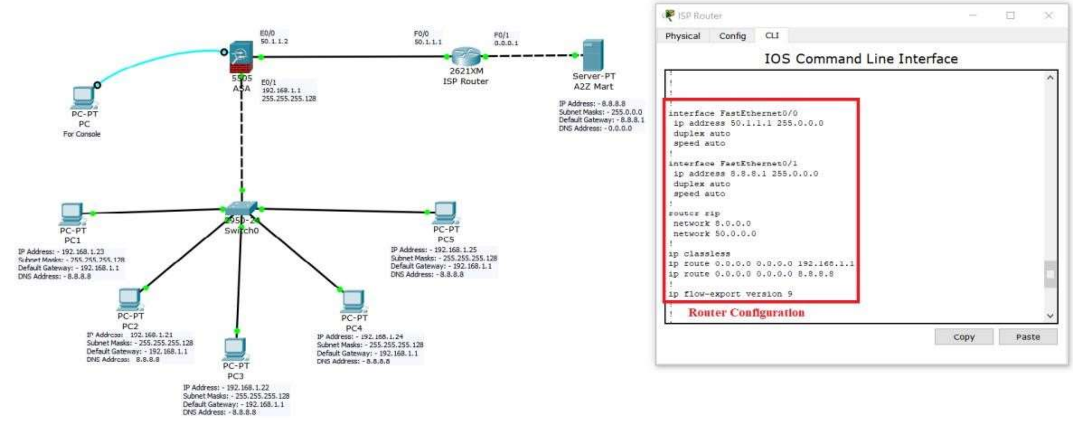


```
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.128
!
interface Vlan2
 nameif outside
```

Firewall Configuration

```
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.128
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 50.1.1.2 255.0.0.0
!
object network LAN
 subnet 192.168.1.0 255.255.255.128
!
route outside 0.0.0.0 0.0.0.0 50.1.1.1 1
!
access-list oti extended permit tcp any any
access-list oti extended permit icmp any any
!
!
access-group oti in interface outside
object network LAN
 nat (inside,outside) dynamic interface
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd address 192.168.1.21-192.168.1.121 inside
dhcpd dns 8.8.8.8 interface inside
dhcpd enable inside
!
```

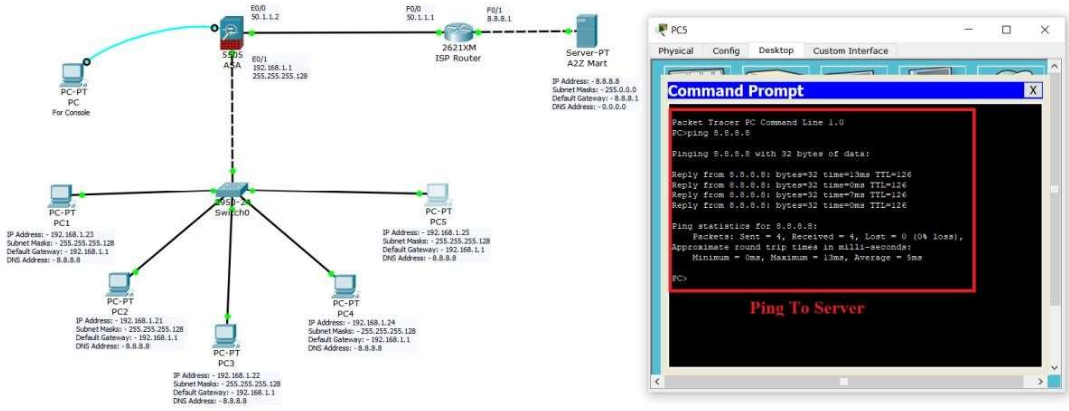
FIREWALL CONFIGURATION


E0/0
50.1.1.2
E0/1
192.168.1.1
255.255.255.128
5505
ASA
F0/0
50.1.1.1
F0/1
8.8.8.1
2621XM
ISP Router
Server-PT
A2Z Mart
IP Address: - 8.8.8.8
Subnet Masks: - 255.0.0.0
Default Gateway: - 8.8.8.1
DNS Address: - 0.0.0.0
PC-PT
PC
For Console
2950-24
Switch0
PC-PT
PC1
IP Address: - 192.168.1.23
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC2
IP Address: - 192.168.1.21
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC3
IP Address: - 192.168.1.22
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC4
IP Address: - 192.168.1.24
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC5
IP Address: - 192.168.1.25
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
ISP Router
Physical
Config
CLI
IOS Command Line Interface
Copy
Paste

```
!
!
!
interface FastEthernet0/0
 ip address 50.1.1.1 255.0.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 8.8.8.1 255.0.0.0
 duplex auto
 speed auto
!
router rip
 network 8.0.0.0
 network 50.0.0.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip route 0.0.0.0 0.0.0.0 8.8.8.8
!
ip flow-export version 9
!
```

Router Configuration

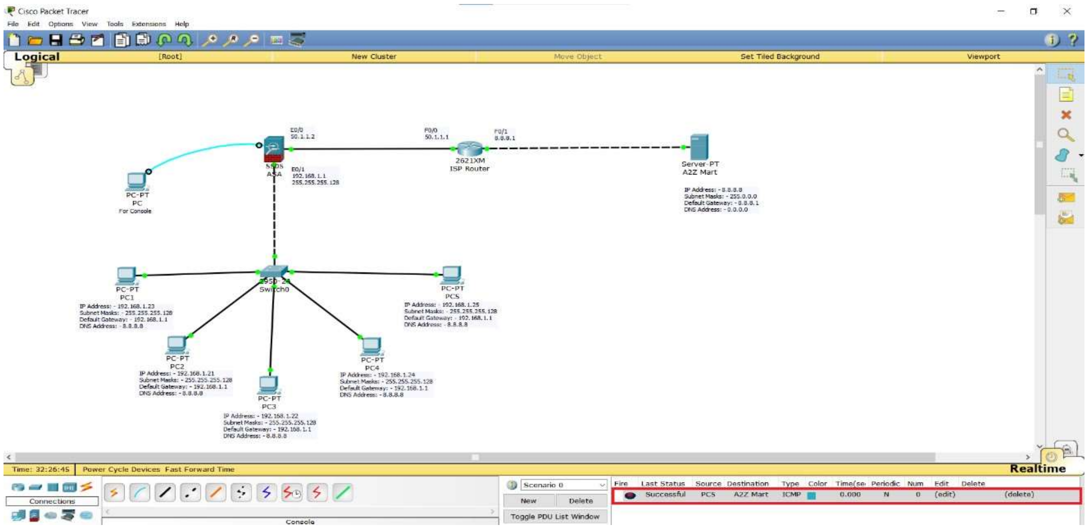
ROUTER CONFIGURATION


E0/0
50.1.1.2
E0/1
192.168.1.1
255.255.255.128
5505
ASA
F0/0
50.1.1.1
F0/1
8.8.8.1
2621XM
ISP Router
Server-PT
A2Z Mart
IP Address: - 8.8.8.8
Subnet Masks: - 255.0.0.0
Default Gateway: - 8.8.8.1
DNS Address: - 0.0.0.0
PC-PT
PC
For Console
2950-24
Switch0
PC-PT
PC1
IP Address: - 192.168.1.23
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC2
IP Address: - 192.168.1.21
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC3
IP Address: - 192.168.1.22
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC4
IP Address: - 192.168.1.24
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC5
IP Address: - 192.168.1.25
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC5
Physical
Config
Desktop
Custom Interface
Command Prompt
X

```
Packet Tracer PC Command Line 1.0
PC>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=13ms TTL=126
Reply from 8.8.8.8: bytes=32 time=0ms TTL=126
Reply from 8.8.8.8: bytes=32 time=7ms TTL=126
Reply from 8.8.8.8: bytes=32 time=0ms 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 = 13ms, Average = 5ms

PC>
```

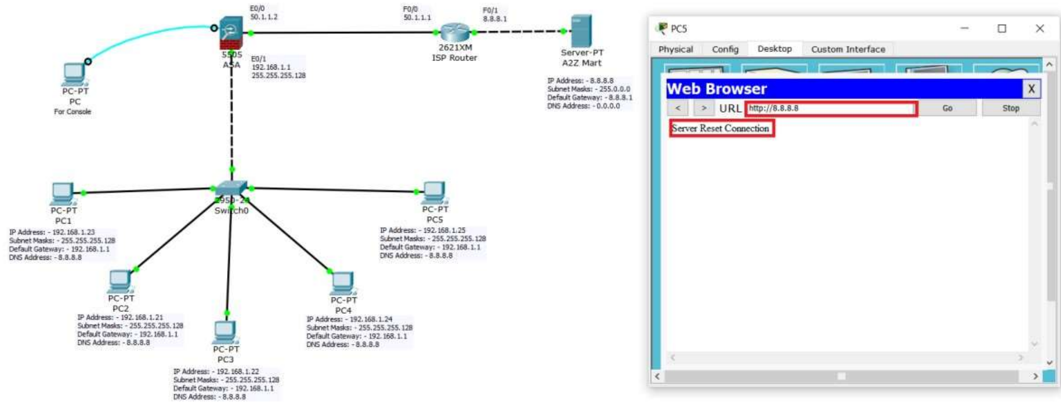
Ping To Server

PING TO SERVER


Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
E0/0
50.1.1.2
E0/1
192.168.1.1
255.255.255.128
5505
ASA
F0/0
50.1.1.1
F0/1
8.8.8.1
2621XM
ISP Router
Server-PT
A2Z Mart
IP Address: - 8.8.8.8
Subnet Masks: - 255.0.0.0
Default Gateway: - 8.8.8.1
DNS Address: - 0.0.0.0
PC-PT
PC
For Console
2950-24
Switch0
PC-PT
PC1
IP Address: - 192.168.1.23
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC2
IP Address: - 192.168.1.21
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC3
IP Address: - 192.168.1.22
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC4
IP Address: - 192.168.1.24
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC5
IP Address: - 192.168.1.25
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
Time: 32:26:45
Power Cycle Devices Fast Forward Time
Realtime
Connections
Console
Scenario 0
New
Delete
Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(se	Periodic	Num	Edit	Delete
●	Successful	PC5	A2Z Mart	ICMP	🟦	0.000	N	0	(edit)	(delete)

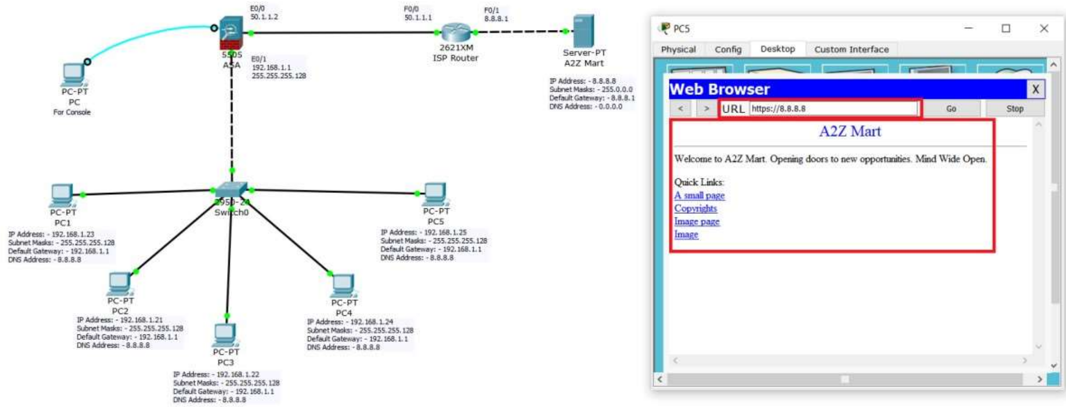
Message to Server


E0/0
50.1.1.2
F0/0
50.1.1.1
F0/1
8.8.8.1
5505
ASA
E0/1
192.168.1.1
255.255.255.128
2621XM
ISP Router
Server-PT
A2Z Mart
IP Address: - 8.8.8.8
Subnet Masks: - 255.0.0.0
Default Gateway: - 8.8.8.1
DNS Address: - 0.0.0.0
PC-PT
PC
For Console
2950-24
Switch0
PC-PT
PC1
IP Address: - 192.168.1.23
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC5
IP Address: - 192.168.1.25
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC2
IP Address: - 192.168.1.21
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC4
IP Address: - 192.168.1.24
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC3
IP Address: - 192.168.1.22
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC5
Physical
Config
Desktop
Custom Interface
Web Browser
X
<
>
Go
Stop

URL http://8.8.8.8

Server Reset Connection

Website Access without HTTPS


E0/0
50.1.1.2
F0/0
50.1.1.1
F0/1
8.8.8.1
5505
ASA
E0/1
192.168.1.1
255.255.255.128
2621XM
ISP Router
Server-PT
A2Z Mart
IP Address: - 8.8.8.8
Subnet Masks: - 255.0.0.0
Default Gateway: - 8.8.8.1
DNS Address: - 0.0.0.0
PC-PT
PC
For Console
2950-24
Switch0
PC-PT
PC1
IP Address: - 192.168.1.23
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC5
IP Address: - 192.168.1.25
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC2
IP Address: - 192.168.1.21
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC4
IP Address: - 192.168.1.24
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC-PT
PC3
IP Address: - 192.168.1.22
Subnet Masks: - 255.255.255.128
Default Gateway: - 192.168.1.1
DNS Address: - 8.8.8.8
PC5
Physical
Config
Desktop
Custom Interface
Web Browser
X
<
>
Go
Stop

URL https://8.8.8.8

A2Z Mart

Welcome to A2Z Mart. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Website Access With HTTPS

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-generationhttps://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-dmz-00.htmlfirewalls/115904-asa-config-dmz-00.html
4. https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-defaulthttps://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-default-routing-in-cisco-routers.htmlrouting-in-cisco-routers.html
5. https://www.computernetworkingnotes.com/ccna-study-guide/static-routinghttps://www.computernetworkingnotes.com/ccna-study-guide/static-routing-configuration-guide-with-examples.htmlconfiguration-guide-with-examples.html
6. https://www.cisco.com/c/dam/assets/sol/sb/isa500_emulator/help/guide/ad1681599.html
7. https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-350-series-managedhttps://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-350-series-managed-switches/smb2942-configure-customer-premises-equipment-cpe-to-a-virtual-local.htmlswitches/smb2942-configure-customer-premises-equipment-cpe-to-a-virtual-local.html
8. https://www.youtube.com/watch?v=jOYvI6aBVE8