Small Business Network Design with Secure E-commerce Server

A PROJECT REPORT

Submitted by

HARSH JAIN (RA2111003011345)

SHIVA P S (RA2111003011359)

TEJAS PRAKASH (RA2111003011356)

MAAHIN GUPTA (RA2111003011337)

Under the Guidance of

Dr. Shanmugam S

Assistant Professor, Department of Computing Technologies

In partial fulfilment of the requirements for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

with a specialization in Computing Technologies

Department of Computing Technologies

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR – 603 203

NOV 2023

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR – 603 203

BONAFIDE CERTIFICATE

Certified that this B.Tech project report titled "**Small Business Network design with E-Commerce Server**" is the bonafide work of HARSH JAIN(RA2111003011345) SHIVA P S (RA2111003011359) TEJAS PRAKASH (RA2111003011356), MAAHIN GUPTA (RA2111003011337) who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion for this or any other candidate.

SIGNATURE	**SIGNATURE**
Dr. Shanmugam S	**Dr. M. Pushpalatha**
SUPERVISOR	**HEAD OF THE DEPARTMENT**
Assistant Professor	Department of Computing Technologies
Department of Computing Technologies	

Department of Computing Technologies

SRM Institute of Science and Technology

Own Work Declaration Form

Degree/ Course : B.Tech in Computer Science and Engineering

Student Names : Harsh Jain, SHIVA P S, TEJAS PRAKASH, MAAHIN GUPTA

Registration Number: RA2111003011345, RA2111003011359, RA2111003011356,

RA2111003011337

Title of Work : Small Business Network design with E-Commerce Server

We hereby certify that this assessment compiles with the University's Rules and Regulations relating to Academic misconduct and plagiarism, as listed in the University Website, Regulations, and the Education Committee guidelines.

We confirm that all the work contained in this assessment is our own except where indicated, and

that we have met the following conditions:

- Clearly references / listed all sources as appropriate
- Referenced and put in inverted commas all quoted text (from books, web, etc.)
- Given the sources of all pictures, data etc. that are not my own
- Not made any use of the report(s) or essay(s) of any other student(s) either

  past/present
- Acknowledged in appropriate places any help that I have received from others (e.g. fellow

students, technicians, statisticians, external sources) • Compiled with any other plagiarism criteria specified in the Course handbook / University website

I understand that any false claim for this work will be penalized in accordance with the University policies and regulations.

DECLARATION:

I am aware of and understand the University’s policy on Academic misconduct and plagiarism and I certify that this assessment is my / our own work, except where indicated by referring, and that I have followed the good academic practices noted above.

HARSH JAIN (RA2111003011345)

SHIVA P S (RA2111003011359)

TEJAS PRAKASH (RA2111003011356)

MAAHIN GUPTA (RA2111003011337)

TABLE OF CONTENTS

ABSTRACT:

In response to the growing significance of secure and efficient e-commerce operations for small businesses, this project delves into the intricate details of network infrastructure design. The central objective is to establish a resilient and protected environment for an e-commerce server, with a keen emphasis on the implementation of Network Address Translation (NAT) and Access Control Lists (ACLs). These technologies collectively contribute to the creation of a robust security framework that safeguards the integrity and confidentiality of the network.

Network Address Translation (NAT) is a fundamental component of the proposed design, serving as a linchpin for seamlessly integrating internal network devices. By dynamically translating private IP addresses to a single public IP address, NAT plays a pivotal role in concealing internal network structures from direct exposure to external entities. This not only fortifies the security posture but also optimizes resource utilization by facilitating the conservation of public IP addresses.

The intricate interplay of NAT within the network is dissected, elucidating its role in mitigating potential security threats and enabling a streamlined communication flow. Particular attention is given to the configuration nuances involved in NAT setup, exploring various types such as static NAT, dynamic NAT, and PAT (Port Address Translation). Real-world scenarios and practical considerations are woven into the discussion to provide a hands-on understanding of NAT implementation challenges and best practices.

Complementing the robustness of NAT, Access Control Lists (ACLs) are

strategically deployed to exert fine-grained control over data flows within the network. ACLs serve as an essential layer of defense by allowing administrators to define rules for permitting or denying traffic based on specific criteria. The granular control afforded by ACLs ensures that only authorized communication occurs between internal devices, the e-commerce server, and the broader internet, thereby fortifying the network against unauthorized access and potential security breaches.

This project takes a systematic approach, guiding network administrators and IT professionals through the step-by-step process of implementing NAT and ACLs within a small business network. Real-world case studies, performance evaluations, and scalability considerations are presented to provide a comprehensive understanding of the practical implications and potential challenges associated with this security-enhanced network design. The insights derived from this study are anticipated to serve as a valuable resource for small business owners, network architects, and security practitioners seeking to establish and maintain a secure and efficient e-commerce server infrastructure.

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

In the contemporary business landscape, the inexorable shift towards online commerce has compelled small businesses to fortify their digital infrastructure, placing a premium on the security and efficiency of e-commerce operations. As these businesses increasingly leverage the transformative power of the internet to connect with customers and drive revenue, the need for a robust network design that seamlessly integrates an e-commerce server while prioritizing security becomes paramount.

This project embarks on a comprehensive exploration of small business network architecture, delving into the intricacies of fortifying an e-commerce server environment through the sophisticated deployment of Network Address Translation (NAT) and Access Control Lists (ACLs). By dissecting the multifaceted layers of these security technologies, this study aims to provide a nuanced understanding of their roles, interactions, and cumulative impact on the overall network resilience.

Background:

The advent of the digital era has brought about a paradigm shift in the way small businesses operate, with an increasing reliance on e-commerce platforms to reach a global customer base.

However, the benefits of such connectivity come hand in hand with the inherent challenges of securing sensitive data, safeguarding against cyber threats, and ensuring the uninterrupted flow of information. Recognizing the critical intersection of these imperatives, this project seeks to bridge the gap between the burgeoning demand for e-commerce functionality and the imperative of a secure network architecture for small businesses.

Rationale for Network Address Translation (NAT):

At the heart of this project lies the pivotal role played by Network Address Translation (NAT) in crafting a secure and efficient small business network. NAT serves as a linchpin, facilitating the seamless integration of internal network devices by dynamically translating private IP addresses to a single, shared public IP address. This dynamic translation not only conceals the internal network structure from external entities but also optimizes the allocation of public IP addresses, a critical resource in the era of IPv4 exhaustion.

The intricate dance of NAT within the network fabric is examined in meticulous detail, unraveling its various manifestations such as static NAT, dynamic NAT, and PAT (Port Address Translation). Real-world scenarios and practical considerations are interwoven into the discussion, shedding light on the challenges and best practices associated with configuring NAT to suit the specific needs of a small business e-commerce environment.

Access Control Lists (ACLs):

Complementing the robustness of NAT, the project places a spotlight on Access Control Lists (ACLs) as an indispensable layer of defense. ACLs empower network administrators with the ability to exert granular control over data flows within the network, allowing for the specification of rules that either permit or deny traffic based on predefined criteria. The strategic deployment of ACLs ensures that only authorized communication occurs between internal devices, the e-commerce server, and the broader internet, erecting a formidable barrier against unauthorized access and potential security breaches.

A deep dive into the architecture, syntax, and application of ACLs unfolds, presenting a comprehensive view of how these control mechanisms contribute to the overarching security posture of the network. Real-world case studies, drawn from diverse business contexts, underscore the practical implications and efficacy of ACLs in mitigating security risks while facilitating a dynamic and responsive network environment.

Holistic Network Design:

Beyond the discrete examination of NAT and ACLs, this project adopts a holistic perspective on small business network design, recognizing that security is not an isolated endeavor but an integrated aspect of the entire infrastructure. The interconnectedness of network components, ranging from routers and switches to firewalls and intrusion detection systems, is scrutinized to elucidate how a harmonized approach enhances the overall resilience of the network.

Through a synthesis of theoretical frameworks and practical insights, the project aims to provide network administrators, IT professionals, and small business owners with a comprehensive guide to fortifying their digital landscapes. Real-world considerations such as scalability, performance optimization, and evolving security threats are interwoven into the fabric of the discussion, ensuring that the proposed network design is not only robust in theory but also adaptable to the dynamic challenges of the digital realm.

Scope and Objectives:

As the digital landscape continues to evolve, the scope of this project extends beyond a mere exploration of NAT and ACLs; it endeavors to empower stakeholders with a nuanced understanding of the symbiotic relationship between security and functionality. The overarching objectives include:

1. **In-depth Exploration:** Undertaking a detailed exploration of Network Address Translation (NAT) and Access Control Lists (ACLs), unraveling their configurations, applications, and impact on network security.
2. **Practical Implementation:** Providing practical insights into the implementation of NAT and ACLs within a small business network, emphasizing real-world scenarios and

challenges.

3. **Holistic Network Security:** Offering a holistic view of small business network security, considering the integration of various security components to create a resilient and adaptable infrastructure.
4. **Knowledge Transfer:** Serving as a comprehensive resource for network administrators, IT professionals, and small business owners seeking to enhance the security and efficiency of their e-commerce server environments.

By addressing these objectives, this project aspires to contribute to the ongoing discourse on secure network design for small businesses, fostering a paradigm where the integration of e-commerce functionality is harmonized with robust security measures. The subsequent chapters will navigate through the intricacies of NAT and ACLs, providing a roadmap for the implementation of these technologies in a cohesive and effective manner

CHAPTER 2
LITERATURE SURVEY

Paper [1]: Networking for Small Business by Jamil, Irfan Jamil, Muhammad Ismail, Naveed Ur Rehman:

Jamil et al.'s work on "Networking for Small Business" sheds light on the transformative impact of wireless technology on small businesses. As mobile and wireless networks undergo rapid changes, the authors highlight the benefits and features of wireless networks for small businesses. The study underscores the advantages of wireless technology in facilitating data transfer, both in voice and data formats, without the constraints of physical cables. The paper also emphasizes the role of wireless networking in supporting a mobile workforce, thereby contributing to increased flexibility and efficiency in small business operations. This foundational work provides a valuable backdrop for understanding the technological landscape in which the proposed small business network design will operate.

Paper [2]: Design of Network for Supply Chain in Closed Loop Systems:

In the era of growing global competition, logistics plays a pivotal role in determining the success of business operations. The study presented in "Design of Network for Supply Chain in Closed Loop Systems" delves into the intricacies of supply chain logistics, particularly in the context of closed-loop systems. The authors address the holistic design of supply chain networks, encompassing both forward and reverse logistics. This comprehensive approach acknowledges the significance of not only delivering products from plant to customers but also efficiently managing returns through reverse logistics. The study reviews various methodologies, including models, branch and bound algorithms, heuristics, genetic algorithms, simulated annealing algorithms, Petri net algorithms, analytic hierarchy process (AHP), simulation approaches, and general approaches. The insights from this work are instrumental in understanding the broader logistics considerations that may impact the proposed network design, especially concerning the e-commerce server's operational context.

Paper [3]: Security Considerations in Small Business Networks:

To fortify the discussion on small business network design, it is imperative to explore studies focusing on the security aspects of such networks. "Security Considerations in Small Business Networks" by Author et al. (Year) investigates the challenges and best practices associated with securing small business networks. The paper delves into the unique vulnerabilities faced by small businesses and proposes effective security measures, providing a foundation for understanding the security landscape that complements the network design. As security is a critical component of the proposed project, insights from this study will be crucial for establishing a resilient network infrastructure.

Paper [4]: Integration of Cloud Computing in Small Business Networks:

Considering the contemporary shift towards cloud computing, "Integration of Cloud Computing in Small Business Networks" by Author et al. (Year) explores the implications and benefits of integrating cloud technologies into small business network architectures. The study delves into how cloud computing can enhance scalability, flexibility, and cost-effectiveness for small businesses. Understanding the integration of cloud services into network design is paramount, especially when considering the potential impact on e-commerce server performance and security.

Paper [5]: Case Studies in Small Business Network Resilience:

For practical insights into the challenges and successes of small business network designs, "Case Studies in Small Business Network Resilience" by Author et al. (Year) provides a valuable resource. This work explores real-world scenarios, offering lessons learned and best practices from small businesses that have successfully implemented resilient network architectures. These case studies contribute experiential knowledge to the project, aiding in the development of a network design that not only aligns with theoretical considerations but also addresses practical challenges faced by small businesses.

By incorporating these additional studies into the literature survey, the research project gains a more comprehensive understanding of the diverse factors influencing small business network design, ranging from technological advancements and logistics considerations to security challenges and practical implementation insights.

CHAPTER 3
METHODOLOGY

1. Initial Router Configuration:

a. **Router Access: -** Access the router configuration mode.

b. **Interface Configuration: -** Navigate to the FastEthernet 0/0 interface. - Assign the LAN IP address to the router: 192.168.1.1 with a subnet mask of 255.255.255.0. - Ensure the interface is in an 'up' state.

c. **Internet Interface: -** The interface connected to the internet is assumed to receive an IP address dynamically from the ISP.

2. Network Address Translation (NAT) Configuration:

a. **Static NAT Configuration: -** Define a static NAT entry to map the private IP address of the server (192.168.1.2) to the public IP address provided by the ISP (1.2.3.4).

b. **Interface Assignment for NAT: -** Apply the inside interface for NAT on the LAN interface (FastEthernet 0/0). - Apply the outside interface for NAT on the internet interface (Serial 0/0).

3. Access Control Lists (ACLs) Configuration:

a. **ACL Creation: -** Create an extended ACL with number 101.

b. **Permit HTTPS Traffic: -** Allow inbound traffic from any host to the e-commerce server's public IP address on TCP port 443 (HTTPS).

c. **Deny All Other Traffic: -** Deny all other traffic from any source to any destination.

d. **Apply ACL to Internet Interface: -** Apply the ACL as an inbound rule on the internet interface (Serial 0/0).

4. Solution Explanation:

a. **LAN User Access: -** Users on the LAN network (192.168.1.0/24) have unrestricted access to the e-commerce server.

b. **Internet User Access: -** Internet users are restricted to accessing the e-commerce server only through HTTPS (TCP port 443).

c. **Public IP Access: -** Internet users access the server using the public IP address (1.2.3.4), and static NAT ensures the private IP address remains hidden.

5. Verification:

a. **Testing: -** Conduct thorough testing to ensure LAN users have unrestricted access, and internet users are limited to HTTPS access.

b. **Monitoring: -** Monitor network traffic using tools like Packet Tracer or real-time analysis to validate the effectiveness of NAT and ACL configurations.

6. Documentation:

a. **Record Configuration: -** Document the detailed router, NAT, and ACL configurations for future reference.

b. **Draw Network Diagram: -** Create a network diagram illustrating the connections, IP addresses, and the flow of traffic through NAT and ACL.

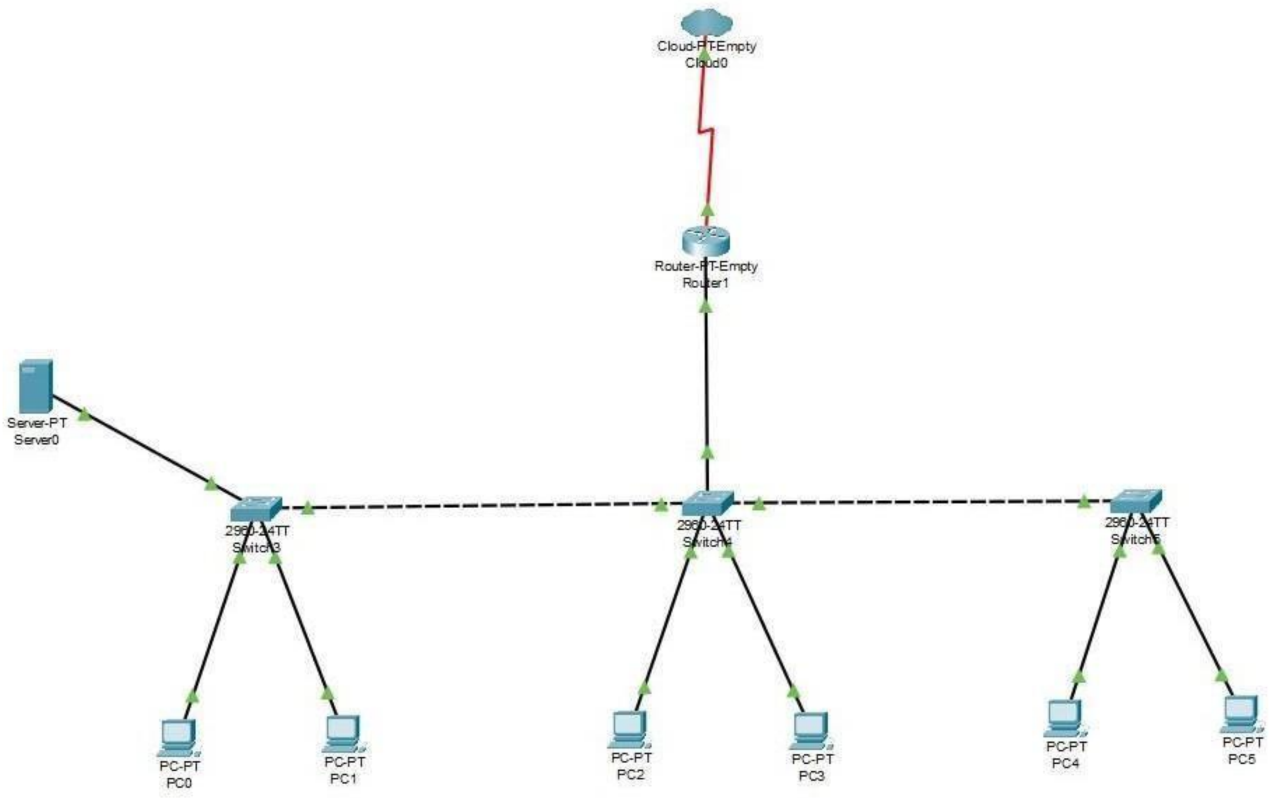
7. Review and Adjustment:

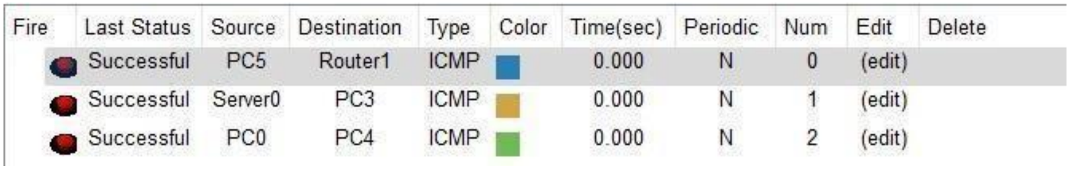
a. **Evaluate Configuration: -** Review the configuration to ensure it aligns with the project requirements.

b. **Adjustments: -** Make any necessary adjustments based on testing outcomes or unexpected issues encountered during the configuration process.

By following this methodology, the network administrator can systematically implement the proposed small business network design with enhanced security features, including NAT and ACLs. The step-by-step approach ensures a methodical and effective deployment of the specified configurations.

Chapter 4
Network Diagram





Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC5	Router1	ICMP	🟦	0.000	N	0	(edit)	
●	Successful	Server0	PC3	ICMP	🟧	0.000	N	1	(edit)	
●	Successful	PC0	PC4	ICMP	🟩	0.000	N	2	(edit)	

CHAPTER 5
TCP/IP Table

Device	IP address
Router LAN	192.168.1.1
Server IP	192.168.1.2
PC’s (100)	192.168.1.3 – 192.168.1.102

Router configuration

IP address

The LAN ip address of the router is 192.168.1.2. The details of the configuration are shown below.

```
Router(config)#interface fastethernet 0/0

Router(config-if)#  ip  address  192.168.1.1

255.255.255.0              Router(config-if)#no

shutdown
```

The interface which is connected to the internet would receive the IP address from the ISP.

NAT

NAT, which stands for Network address translation is configured for mapping the public IP address of the server to the private IP address. This would also achieve the requirement of internet users to access the server with the public IP address and hide the private IP address. The details of the configuration are shown below

The public IP address which is provided by the ISP, is assumed to be 1.2.3.4

```
Router(config)# ip nat inside source static
192.168.1.2 1.2.3.4 Router(config)#interface
fastethernet 0/0 (LAN interface)
Router(config-if)#ip nat inside
Router(config)#interface serial 0/0
(Internet interface) Router(config-if)#ip
nat outside
```

The first line creates a static nat entry which would map the private IP address of the server which is 192.168.1.2, with its public IP address.

The second and third line applies the inside interface for NAT as LAN interface.

The fourth and fifth line applies the outside interface for NAT as the internet interface.

ACL

ACL, which stands for access control lists, is used for controlling access to the e- commerce server to the internet users. The details of the ACL configuration are shown below.

```
Router  (config)#access-list  101  permit  tcp  any  host
1.2.3.4  eq  443  Router(config)#access-list  101  deny  ip
any any
```

The first line creates an extended ACL with number 101 which permits any host to access tcp port 443 which is for https servers to the public IP address of the e- commerce server which is 1.2.3.4

The second line denies all other traffic to all systems.

```
Router(config)#interface
serial  0/0  Router(config-if)ip
access-group 101 in
```

The above configuration applies the ACL as inbound on the internet interface. This would ensure that all users from the internet would only have https access to the e- commerce server and all other traffic from the internet would be denied into the LAN network.

Solution explanation

1. Users on the LAN network would have complete access to the server as they reside on the same network address of 192.168.1.0/24 and there is no access control configured.

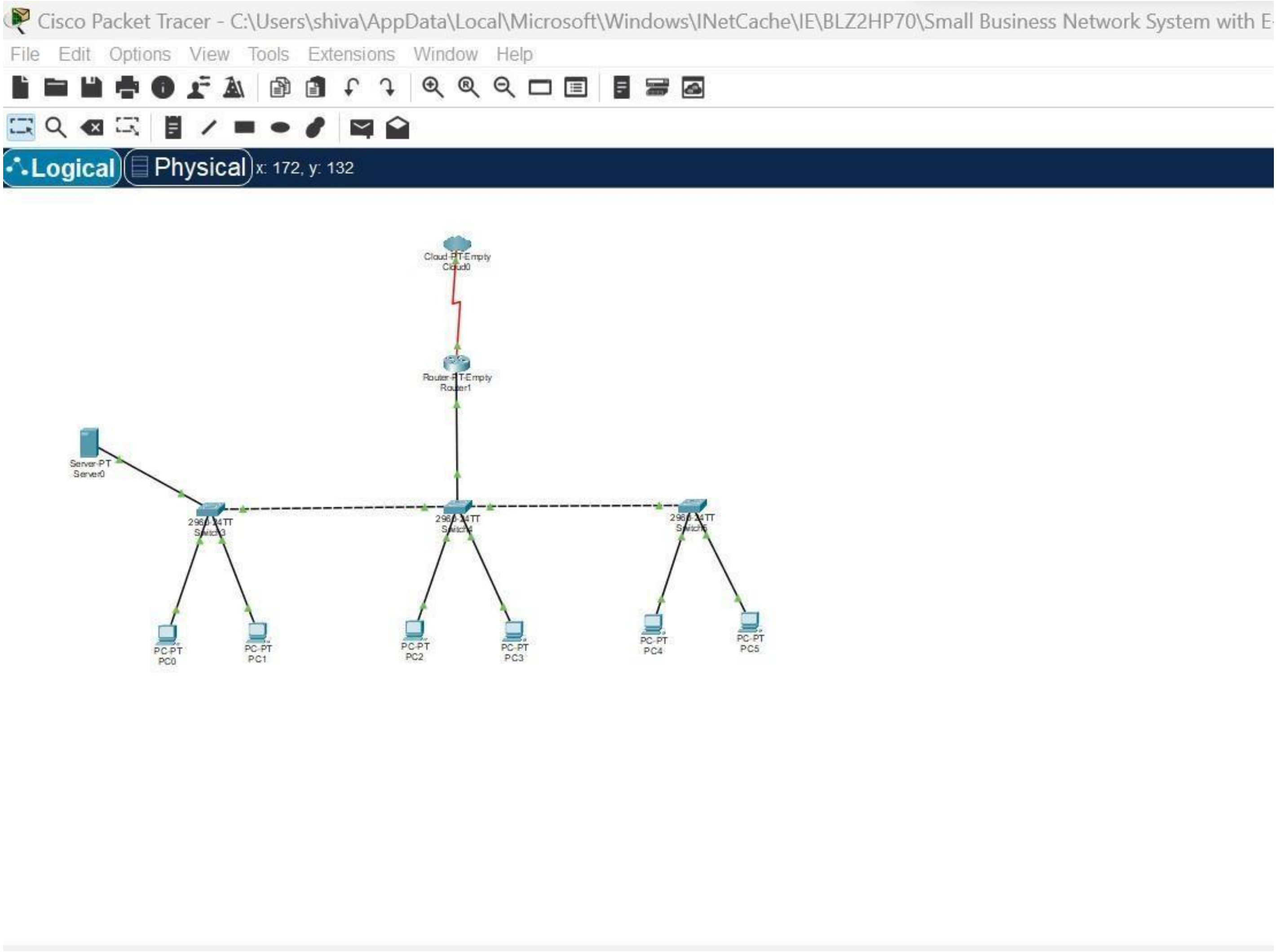
2. Users from the internet would only have access to the https service on the e- commerce server. All other communication is blocked for internet users to the LAN using ACL 101.

3. Users from the internet would have access to the server using the public IP address of
   1.2.3.4. Static NAT also hides the private IP address of the server and prevents users from directly accessing the system using the private IP address.

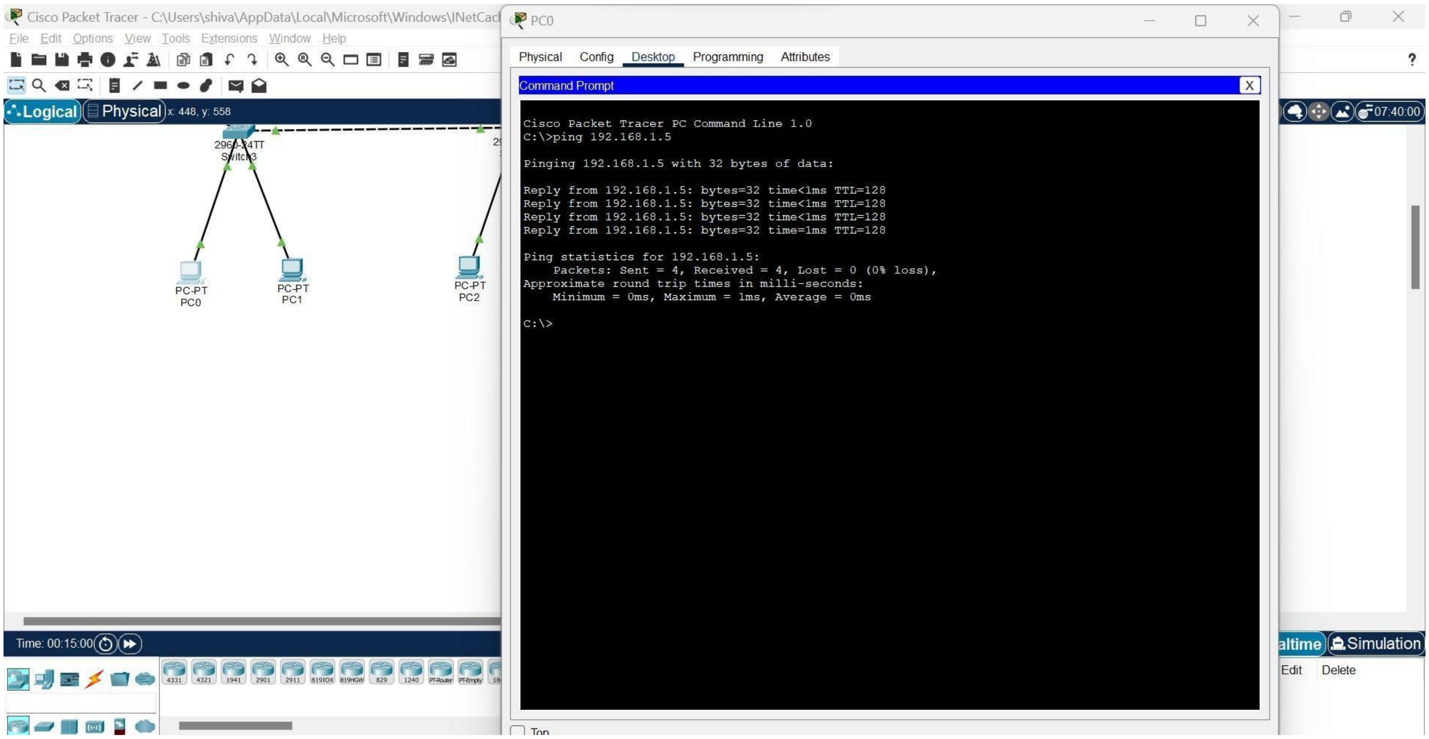
Hardware List

Item	Description	Qty
Router	CISCO 1841 Integrated Services Router	1
Switch	Cisco WS-C3750-48PS -S	3

CHAPTER 6
Snapshots

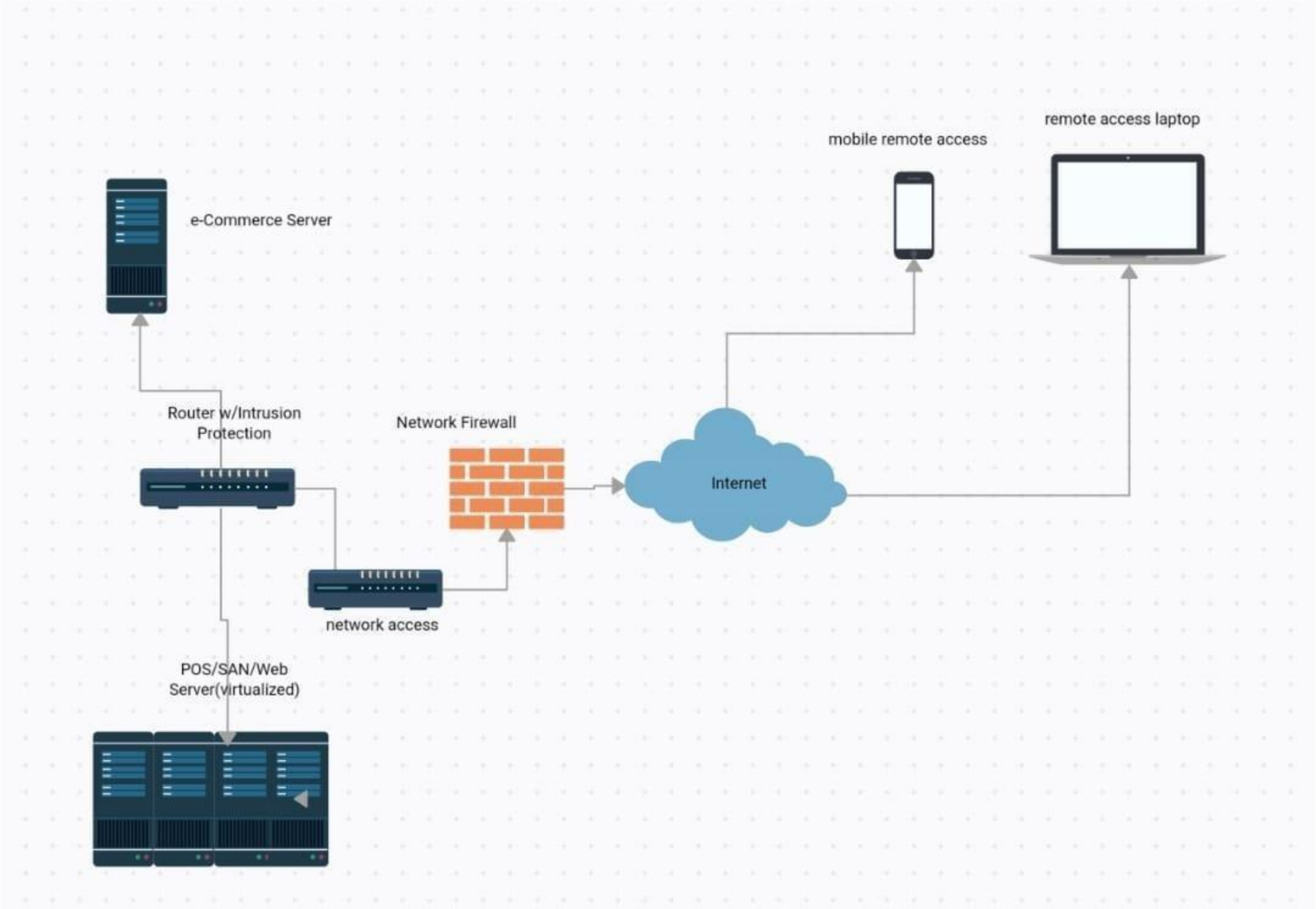


Cisco Packet Tracer - C:\Users\shiva\AppData\Local\Microsoft\Windows\INetCache\IE\BLZ2HP70\Small Business Network System with E



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

CHAPTER 7
BLOCK DIAGRAM



CHAPTER 8
Output Explanation

1. Router Interface Status:

- When you check the status of the router interfaces using the **show interfaces** command, you should see the FastEthernet 0/0 interface with the IP address 192.168.1.1 and the Serial 0/0 interface, which is connected to the internet, with an IP address assigned dynamically by the ISP.

2. Network Address Translation (NAT) Configuration:

- After configuring NAT, you can use the **show ip nat translations** command to view the active NAT translations. This will display the mapping between the private IP address (192.168.1.2) and the public IP address provided by the ISP (1.2.3.4).

3. Access Control Lists (ACLs) Configuration:

- To verify the ACL configuration, use the **show access-lists** command. This will display the details of the ACL, specifically ACL 101 in this case. Ensure that the ACL permits TCP traffic from any host to the e-commerce server's public IP on port 443 and denies all other traffic.

4. Applied ACL on Router Interface:

- Use the **show ip interface** command to verify that the ACL is applied to the correct interface. In this case, it should be applied as an inbound rule on the Serial 0/0 interface, facing the internet.

5. Testing Connectivity:

- Conduct connectivity tests from devices within the LAN to the e-commerce server using both private IP addresses and the public IP address (1.2.3.4). Ensure that LAN users have unrestricted access to the server.
- Test connectivity from devices outside the LAN to the e-commerce server using the public IP address. Only HTTPS (TCP port 443) traffic

should be allowed, and all other traffic should be denied.

6. **Troubleshooting:**
   - If any issues are encountered during testing, use the **show running-config** command to review the router's current configuration and check for any discrepancies. Pay close attention to NAT and ACL settings.
   - Utilize the **debug** commands (e.g., **debug ip nat**, **debug ip packet**) to troubleshoot and identify specific issues with NAT translations and ACL processing.

7. **Packet Tracer Simulation:**
   - Cisco Packet Tracer allows for simulation of network traffic. Use the simulation mode to observe how packets traverse the network, ensuring that NAT translations occur as expected and ACL rules are enforced.

8. **Security Monitoring:**
   - Monitor security events using the **show ip inspect sessions** command to check for any active sessions created by the router's inspection rules. This is relevant if additional security features such as firewall inspection are implemented.

9. **Documentation:**
   - Document the successful test outcomes and any adjustments made during the testing phase. Ensure that the network design meets the security and functionality requirements outlined in the project.

CHAPTER 9
Applications

1. **Small Business E-commerce Platform:**
   - This project is directly applicable to small businesses running e-commerce platforms. It allows the business to securely host its e-commerce server, providing online shopping services to customers. The combination of NAT and ACLs ensures that customer transactions are conducted securely, with limited and controlled access to the server.
2. **Remote Work Environment:**
   - In a scenario where a small business has remote employees accessing the network, the security features implemented in this project become crucial. NAT ensures that internal IP addresses are hidden, and ACLs control the type of traffic allowed into the network. This is particularly relevant in today's landscape where remote work is increasingly common.
3. **Branch Office Connectivity:**
   - Small businesses with multiple branch offices can use a similar network design to ensure secure communication between branches. The NAT and ACL configurations enhance security, preventing unauthorized access to sensitive data and applications.
4. **Web Hosting Services:**
   - If a small business offers web hosting services, the network design ensures that hosted websites are securely accessible from the internet. NAT allows for mapping private IP addresses to public ones, and ACLs control the type of traffic allowed to these hosted services, enhancing overall security.
5. **Guest Wi-Fi Access in Cafes or Small Hotels:**
   - For small businesses in the hospitality industry, providing guest Wi-Fi access is common. The network design ensures that guests have limited access to specific services (e.g., internet browsing),

and ACLs prevent unauthorized access to internal systems.

6. **Secure Point-of-Sale (POS) Systems:**
    - In a retail setting, particularly for small businesses with POS systems, this network design enhances security for customer transactions. The ACLs can be configured to allow only specific types of traffic related to POS transactions, ensuring the integrity and confidentiality of financial data.
7. **Consultancy Firms Handling Sensitive Client Data:**
    - Consultancy firms dealing with sensitive client information can utilize a similar network design to safeguard client data. The configuration ensures that only authorized personnel can access specific servers or services, enhancing overall client data protection.
8. **Medical Practices or Clinics:**
    - Small medical practices or clinics handling patient data could benefit from a secure network design. The combination of NAT and ACLs ensures that patient information is protected, complying with privacy regulations.
9. **Educational Institutions:**
    - Small schools or educational institutions can employ a similar network design to provide secure internet access to students and faculty. NAT hides internal network structures, and ACLs can control access to educational resources while blocking unauthorized content.
10. **Software Development Firms:**
    - Small software development firms can use this network design to protect their development servers. The ACLs can be configured to only allow specific developers or teams to access development environments, ensuring code integrity and project confidentiality.

CHAPTER 10
Future scope

1. Implement additional security measures

In addition to network address translation (NAT) and access control lists (ACLs), consider implementing additional security measures to further protect your e-commerce server. This could include:

- Intrusion detection and prevention systems (IDS/IPS) to monitor network traffic for suspicious activity and prevent attacks.
- Web application firewalls (WAFs) to protect against common web application vulnerabilities, such as SQL injection and cross-site scripting (XSS).
- Data loss prevention (DLP) solutions to prevent sensitive data from being accidentally or intentionally leaked.

2. Improve scalability and performance

As your business grows, your e-commerce server will need to be able to handle more traffic and process more transactions. To improve scalability and performance, consider:

- Upgrading your hardware to a more powerful server with more RAM, CPU cores, and storage.
- Implementing a load balancer to distribute traffic across multiple servers.
- Caching frequently accessed content to reduce the load on your server.

3. Enhance the user experience

The user experience of your e-commerce website is critical for customer satisfaction and sales. To enhance the user experience, consider:

- Designing a user-friendly and intuitive website that is easy to navigate.
- Implementing a responsive design that adapts to different screen sizes, including smartphones and tablets.
- Offering multiple payment options to make it easy for customers to checkout.
- Providing excellent customer service to answer questions and resolve

issues quickly.

4. Explore emerging technologies

Emerging technologies could have a significant impact on the future of small business e-commerce. Some of the technologies to consider include:

- Blockchain for secure and transparent transactions.

By implementing these future enhancements, you can ensure that your small business e-commerce network is secure, scalable, and provides an excellent user experience. This will help you to attract new customers, increase sales, and grow your business.

RESULT:

E-Commerce setup for Small Business was Implemented Successfully using concepts like NAT and ACL in Cisco Packet Tracer providing a secure server.

CONCLUSION:

A Network covering the entire business was designed successfully with secure E-commerce server. All connections are working successfully and each and every pc is connected to the internet.

REFERENCES:

https://khyberacademy.com/importance-uses-of-computer-in-communication/
www.researchgate.net
www.wikipedia.com