MAHATMA GANDHI INSTITUTE OF TECHNOLOGY (Autonomous)

Chaitanya Bharathi (P.O), Gandipet, Hyderabad – 500075

Department of Information Technology

Laboratory Project Report

On

NAME OF PROJECT: Basic Firewall Implementation

COURSE CODE: CS551PC

COURSE NAME: COMPUTER NETWORKS LAB

By

Name of Students:

NITTALA SIVA PRADYUMNA: 23261A3237

NUNAVATH GANESH: 23261A3238

PATI JAHNAVI: 23261A3240

PATLOLLA SAI PAVAN REDDY: 23261A3241

PEDAPUDI RITHIK: 23261A3242

B. TECH SEM Vth

Academic year: 2025-2026

Submission date:

Faculty Instructor

Mrs. V. VEENA

Assistant Professor, Dept of IT, MGIT

Branch : Computer Science and Business system

CERTIFICATE

This is to certify that the project entitled "Basic Firewall Implementation" has been submitted to the Department of Information Technology, Mahatma Gandhi Institute of Technology, for the partial fulfilment of the requirements of the B. Tech Vth Sem Computer Networks Laboratory course done by "NITTALA SIVA PRADYUMNA: 23261A3237, NUNAVATH GANESH: 23261A3238, PATI JAHNAVI:23261A3240, PATLOLLA SAI PAVAN REDDY: 23261A3241, PEDAPUDI RITHIK: 23261A3242" of computer science and Bussiness system.

Project Guide

Mrs. V. Veena

Assistant Professor, Dept of IT, MGIT

INDEX

ABSTRACT

In today's interconnected digital landscape, network security has become a critical concern for organizations of all sizes. The increasing sophistication of cyber threats and the growing dependency on network infrastructure necessitate robust security measures to protect sensitive data and ensure business continuity. This project presents a comprehensive implementation of a secure network architecture using the Cisco ASA 5506-X Firewall in Cisco Packet Tracer.

The primary objective is to design and implement a three-zone security model comprising an Inside Network (trusted zone), a DMZ (Demilitarized Zone for partially trusted servers), and an Outside Network (untrusted zone). The network topology implements industry-standard security practices, including proper segmentation, IP addressing schemes, and security policies.

The Inside Network (192.168.100.0/24) hosts five end-user workstations, the DMZ (10.10.10.0/28) contains critical servers including Web, DNS, DHCP, and Email servers, while the Outside Network (20.20.20.0/24) simulates the external untrusted environment. The Cisco ASA 5506-X Firewall serves as the central security device, configured with appropriate security levels (Inside 100, DMZ 50, Outside 0) to control traffic flow between zones. The implementation includes Network Address Translation (NAT) for Inside-to-Outside communications, Access Control Lists (ACLs) for granular traffic control, and ICMP inspection policies for proper connectivity testing. This project demonstrates practical network security implementation, validates connectivity between different security zones, and provides a foundation for understanding enterprise-level network security architecture. The results show successful segmentation, proper firewall policy enforcement, and controlled inter-zone communication.

INTRODUCTION

Network security is a fundamental requirement for modern organizations to protect their digital assets, maintain data confidentiality, ensure integrity, and guarantee availability of services. With the exponential growth of cyber threats, including malware, ransomware, unauthorized access attempts, and data breaches, implementing robust security measures has become imperative.

Firewall technology forms the cornerstone of network security architecture, acting as a barrier between trusted internal networks and untrusted external networks.

The Cisco Adaptive Security Appliance (ASA) series represents enterprise-grade firewall solutions that provide comprehensive security features, including stateful packet inspection, Virtual Private Network (VPN) capabilities, intrusion prevention, and advanced threat protection.

This project focuses on implementing a three-tier network security architecture using the Cisco ASA 5506-X Firewall within the Cisco Packet Tracer simulation environment. The architecture segregates the network into distinct security zones—the Inside Network (trusted internal users), the DMZ (publicly accessible servers), and the Outside Network (external/Internet), each with appropriate security controls and access policies.

OBJECTIVES

1. Design a secure three-zone network architecture with proper segmentation.

2. Implement the Cisco ASA 5506-X Firewall as the central security device

3. Configure appropriate security levels and policies for each network zone

4. Establish controlled communication between different security zones

5. Implement Network Address Translation (NAT) for Inside-to-Outside connectivity

6. Configure Access Control Lists (ACLs) for granular traffic control

7. Deploy and configure critical servers (Web, DNS, DHCP, Email) in the DMZ

8. Test and validate connectivity and security policies

9. Document the complete implementation process

10. Demonstrate practical understanding of enterprise network security

SYSTEM REQUIREMENTS

Hardware Requirements (For Physical Implementation):

- Cisco ASA 5506-X Firewall (1 unit)
- Cisco Catalyst 2960 Series Switches (3 units)
- End-user workstations/PCs (5 units minimum)
- Server hardware for DMZ services (4 units)
- Category 6 Ethernet cables
- Console cable for device configuration

Simulation Environment:

- Computer with minimum:
- Intel Core i5 or equivalent, 2.0 GHz or higher
- 8 GB RAM minimum (16 GB recommended)
- 10 GB free disk space
- 1366x768 minimum display resolution

- Ethernet adapter

Software Requirements:

- Cisco Packet Tracer 8.0 or higher
- Operating System: Windows 10/11, macOS, or Linux
- Cisco ASA software version 9.8 or higher (included in Packet Tracer)
- Web browser for testing web server connectivity

Network Requirements:

- IP Addressing for each network zone
- Inside Network (trusted zone): 192.168.100.0/24 (5 PCs)
- DMZ (partially trusted): 10.10.10.0/28 (4 servers: Web, DNS, DHCP, Email)
- Outside Network (untrusted zone): 20.20.20.0/24 (2 PCs, 1 Server)
- Bandwidth: Minimum 100 Mbps Ethernet (1 Gbps recommended)

TECHNOLOGIES USED

- Cisco ASA 5506-X Firewall: Enterprise-grade security appliance providing stateful packet inspection, VPN capabilities, NAT, access control lists, and advanced threat protection.

- Cisco Packet Tracer: Network simulation software used to design, configure, and test network topologies virtually.

- Cisco Catalyst 2960 Switches: Used for segmenting network zones and connecting multiple devices.

- Windows 10/11, macOS, Linux: Supported operating systems for running the simulation and associated network services.

- Web, DNS, DHCP, Email Server Services: Emulated in the DMZ environment for realistic network service deployment.

- Ethernet networking (Category 6 cables): Used for physical and simulated network connections.

- Access Control Lists (ACLs): For policy-based traffic control between zones.

- Network Address Translation (NAT): For enabling devices on the inside network to communicate with external networks securely.

IMPLEMENTATION DETAILS

- **Network Topology**: A three-zone security architecture is designed using Cisco Packet Tracer. It consists of an Inside Network (trusted), DMZ (Demilitarized Zone for servers), and an Outside Network (untrusted).

- **Device Placement:**

- Five end-user PCs are placed in the Inside Network.

- Four servers (Web, DNS, DHCP, Email) are placed in the DMZ.

- Two PCs and one server are in the Outside Network.

- **Connections:** Each network zone connects via a Cisco Catalyst 2960 Switch to the Cisco ASA 5506-X Firewall. All network links use straight-through Ethernet cables.

- **IP Addressing**: Each device is assigned a static IP according to its zone:

- Inside: 192.168.100.0/24

- DMZ: 10.10.10.0/28

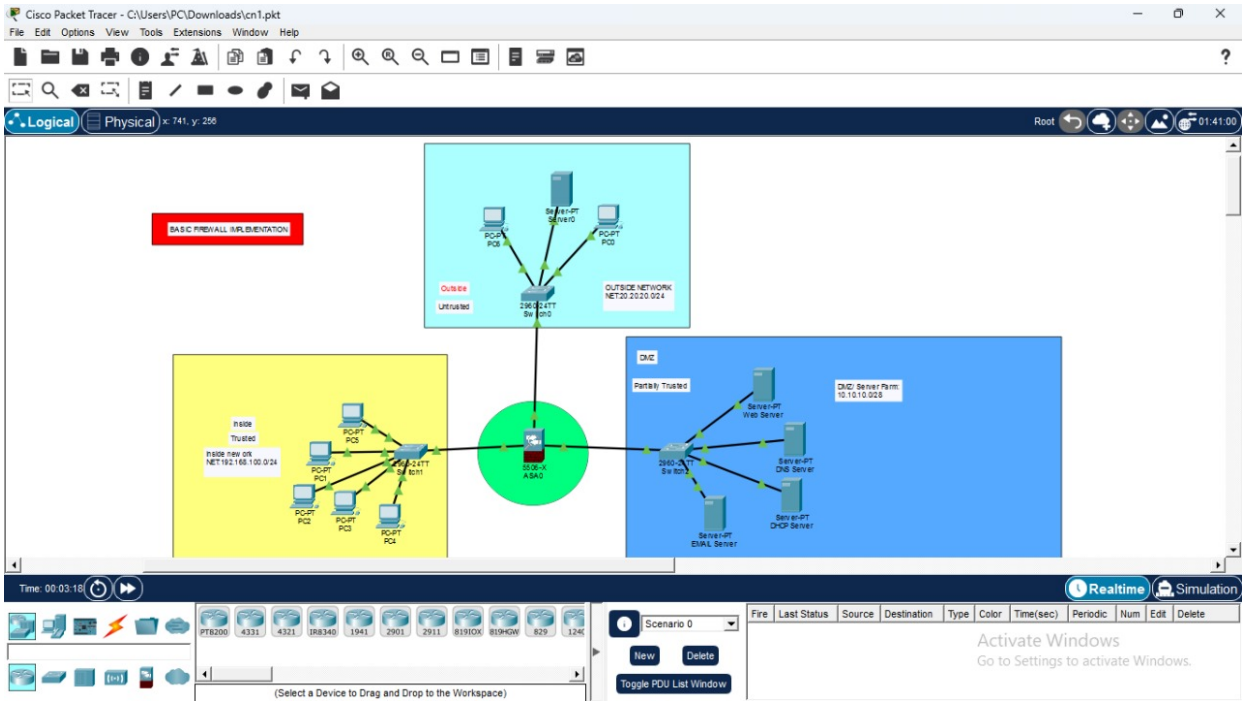
- Outside: 20.20.20.0/24

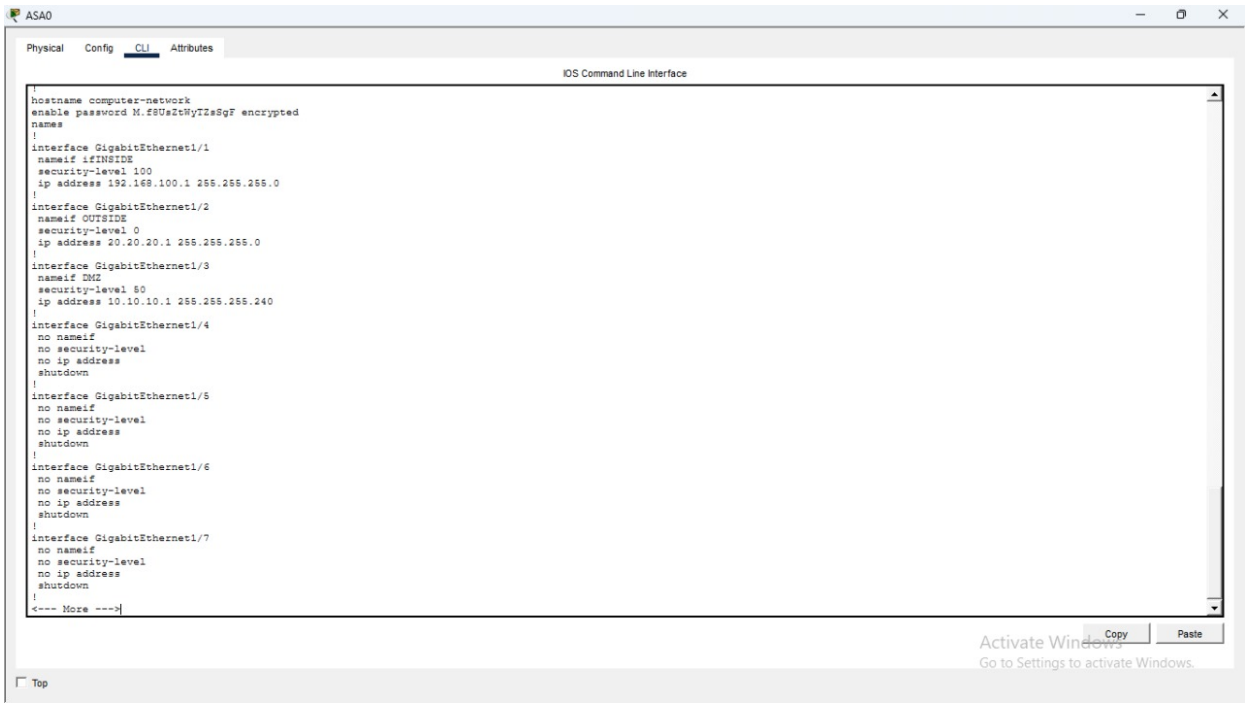
- **ASA Firewall Configuration:**ASA interfaces are configured and assigned to the respective network zones (Inside, DMZ, Outside) with appropriate security levels (Inside 100, DMZ 50, Outside 0).

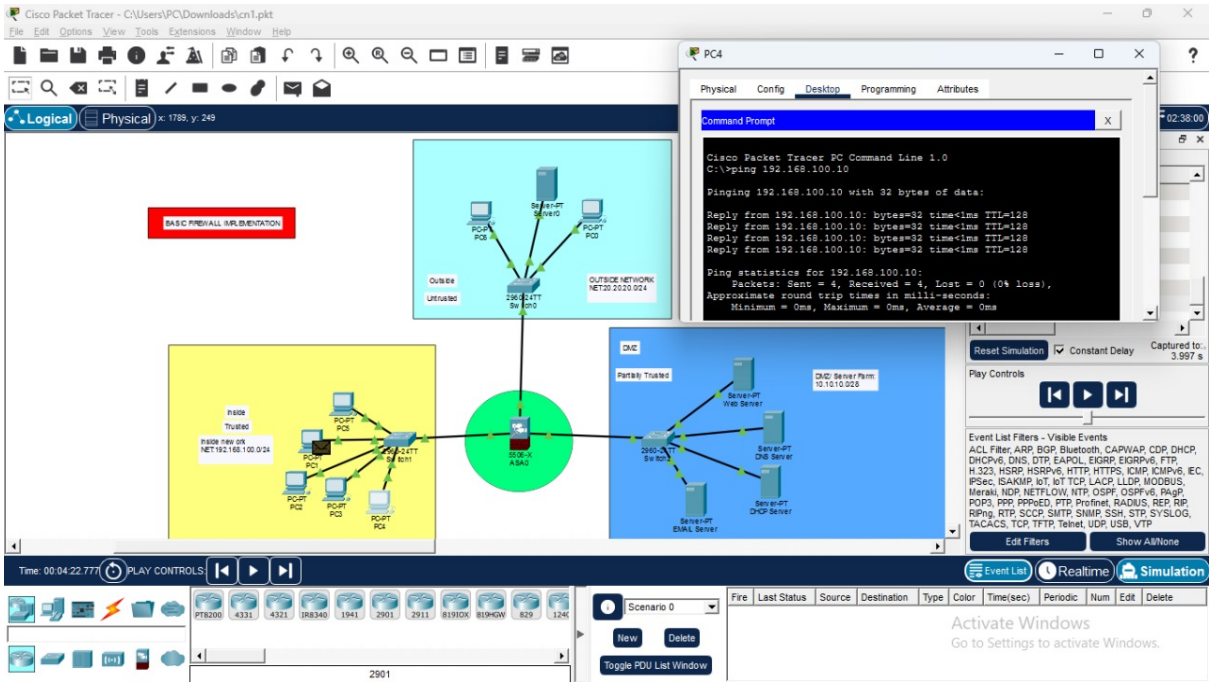
- ICMP inspection is enabled for ping replies.
- Dynamic NAT (PAT) enables inside devices to access the outside network.
- Access Control Lists (ACLs) are configured for traffic control between zones.
- **Server Configuration:**
- DMZ servers are given static IPs and individual services are enabled (DNS, Web, DHCP, Email).
- **Testing:**
- Inside network can access DMZ and the external network, validating NAT and firewall configurations.
- DMZ servers respond to authorized requests.
- Outside network cannot access inside network or DMZ unless explicitly allowed by ACL, proving security isolation.
- **Verification:**
- Firewall and NAT configurations are verified with CLI commands.
- Ping and server access tests confirm connectivity and security enforcement.

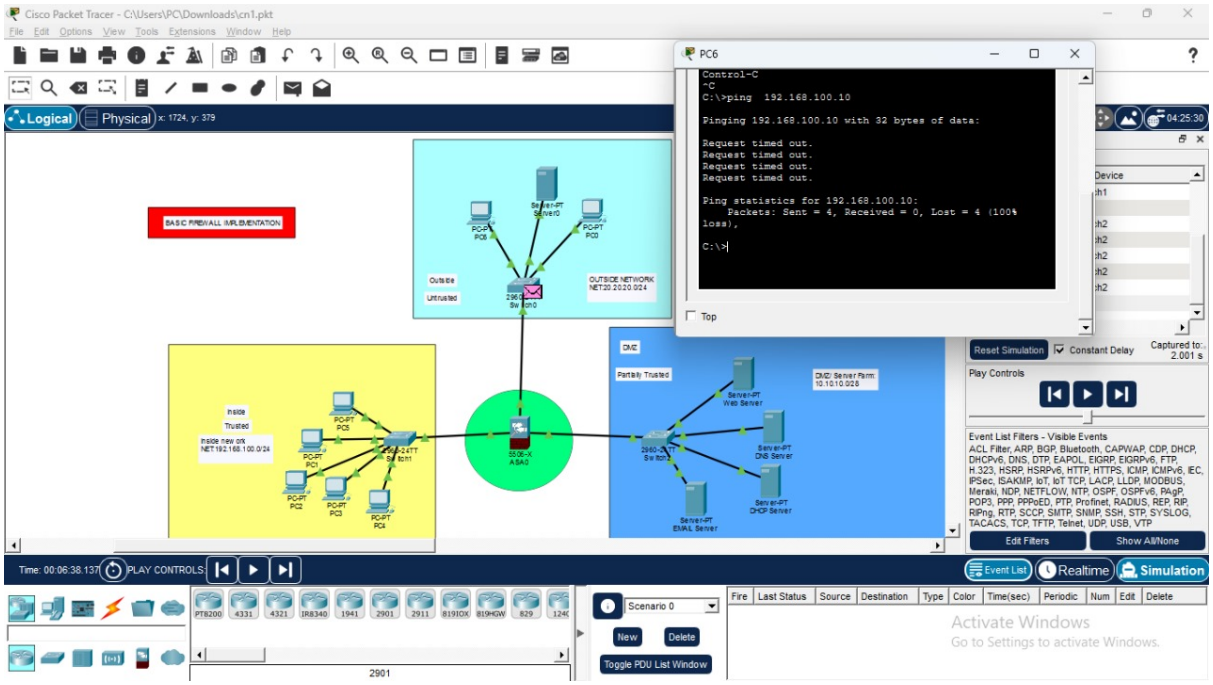
- This ensures robust segmentation, secure policy enforcement, and controlled inter-zone communication within the simulated enterprise network

RESULTS AND OUTPUTS






Cisco Packet Tracer - C:\Users\PC\Downloads\cn1.pkt
PC4
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.10
Pinging 192.168.100.10 with 32 bytes of data:
Reply from 192.168.100.10: bytes=32 time<1ms TTL=128
Reply from 192.168.100.10: bytes=32 time<1ms TTL=128
Reply from 192.168.100.10: bytes=32 time<1ms TTL=128
Reply from 192.168.100.10: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.100.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Logical
Physical
BASIC FIREWALL IMPLEMENTATION
OUTSIDE NETWORK
NET:20.20.20.0/24
DMZ
Server-PT Web Server
Server-PT DNS Server
Server-PT DHCP Server
Server-PT EMAIL Server
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Activate Windows
Go to Settings to activate Windows.


Cisco Packet Tracer - C:\Users\PC\Downloads\cn1.pkt
PC6
Control-C
^C
C:\>ping 192.168.100.10
Pinging 192.168.100.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.100.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top
Logical
Physical
BASIC FIREWALL IMPLEMENTATION
OUTSIDE NETWORK
NET:20.20.20.0/24
DMZ
Server-PT Web Server
Server-PT DNS Server
Server-PT DHCP Server
Server-PT EMAIL Server
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Activate Windows
Go to Settings to activate Windows.

APPLICATIONS

Enterprise Network Security: The three-zone architecture is ideal for corporate environments, protecting internal resources, enabling secure access to company data, and supporting compliance (GDPR, HIPAA, PCI-DSS). It's also suitable for branch offices and educational institutions, providing policy consistency, isolating public-facing services, and supporting secure learning platforms.

Web Server Protection: DMZ placement ensures web servers are publicly accessible without exposing internal networks. This benefits public website hosting, e-commerce platforms (with PCI-DSS compliance), and application servers, containing threats within the DMZ and protecting sensitive data.

Email Server Security: Placing email servers in the DMZ enables safe external communication while shielding internal mail infrastructure. This setup supports corporate messaging, spam/malware scanning at the edge, compliance, and secure mobile or remote access integration.

Remote Access Security: The Cisco ASA platform supports secure site-to-site and remote access VPNs, with IPsec and SSL, for teleworkers and branch connectivity. It offers encrypted tunnels, endpoint assessment, multi-factor authentication, and granular access controls for contractors, employees, and mobile users.

CONCLUSION

The project successfully demonstrates the implementation of a secure network architecture using the Cisco ASA 5506-X Firewall within a simulated environment.

By segmenting the network into Inside, DMZ, and Outside zones and applying industry-standard security policies, it achieves strong protection of internal resources, secure DMZ service hosting, and robust isolation from external threats.

The effectiveness of firewall rules, NAT, and ACLs was validated through comprehensive testing, showing that the architecture supports reliable connectivity, service availability, and security enforcement. The design provides an excellent foundation for enterprise network security and can be adapted for real-world deployments with further enhancements such as advanced ACLs, VPN, and intrusion prevention systems.

REFERENCES

GitHub Topics for Cisco Packet Tracer: A curated collection of GitHub repositories with labs, cheat sheets, and project files built in Packet Tracer, covering topics like RIPv2, OSPF, VLANs, and Subnetting.

- cisco-packet-tracer · GitHub Topics

Packet Tracer Projects on GitHub: A specific repository containing examples of basic labs, CCNP labs, and intrusion detection system setups.

- harshrajbedi/Cisco-Packet-Tracer-Projects - GitHub

Simple and Complex Network Project Tutorials: Articles outlining step-by-step implementations for projects like a Small Office/Home Office (SOHO) network, a secure healthcare network, and a hotel network.

- Simple Networking Project Using Packet Tracer | by Adithya V Menon - Medium