IMPLEMENTATION OF FIREWALL IN CORPORATE ENVIRONMENT

PRASHANT KUMAR[1], AJMAL HASAN[1], COLIN HAMLET ABRAHAM[1], D.VINOTHA[2]
1 B.Tech Students
2 Assiatant Professor
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

PRIST UNIVERSITY, Thanjavur, Tamilnadu

ABSTRACT

The increasing complexity of networks, and the need to make them more open due to the growing emphasis on and attractiveness of the Internet as a medium for business transactions, mean that networks are becoming more and more exposed to attacks, both from without and from within. The search is on for mechanisms and techniques for the protection of internal networks from such attacks. One of the protective mechanisms under serious consideration is the firewall. A firewall protects a network by guarding the points of entry to it.

Firewalls are becoming more sophisticated by the day, and new features are constantly being added, so that, in spite of the criticisms made of them and developmental trends threatening them, they are still a powerful protective mechanism. This journal provides an overview of firewall implementation in a corporate environment.

KEYWORDS

Network Security, Firewall, Internet, Complexity in Network

1.INTRODUCTION

Firewall technology uses the filtering aspect of incoming data to determine what is necessary for intercommunication and what else is not required so that the component can be removed to ensure a smoother web experience. The firewall is responsible to deny unauthorized access to your computer through the internet, hence making the computer impervious to threats on the internet. It acts as a barrier between secured internal networks and outside the untrusted network.

Firewalls are classified into two types 1.)Network layer firewall – this firewall makes decisions based on the source address, destination address and ports in individual IP packets 2.)Application layer firewall – this type of firewall is essentially a host running on proxy servers, which do not permit traffic access directly between networks, hence blocking out most scout programs from finding out the information regarding the device and eliminates many methods to controlling it. A prime example would be “syskey” used to access another computer by establishing a connection between two computers.

2.SIMULATION TOOL

Cisco Packet Tracer :

This is a cross-platform of simulation in visual forefront application used to simulate the events transpiring in an interconnected network of computers and various other devices. It is very similar to GNS3. The software allows users to create network topologies and imitate modern computers networks. It also replicates the possible states inside the connections and figures out the current state of the device if it were working in real-time. The simulation tool is very popular in the field of telecommunications and in the field of networking since the software can emulate the various states of many communication devices and its interconnections.

The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Cisco packet tracer can also understand whether the connections between the terminals shall be successful or whether they can be successfully established, this comes into play when the components for this connected environment is very expensive to consider. Hence already preconfigured connection is preferred

3. IMAGE

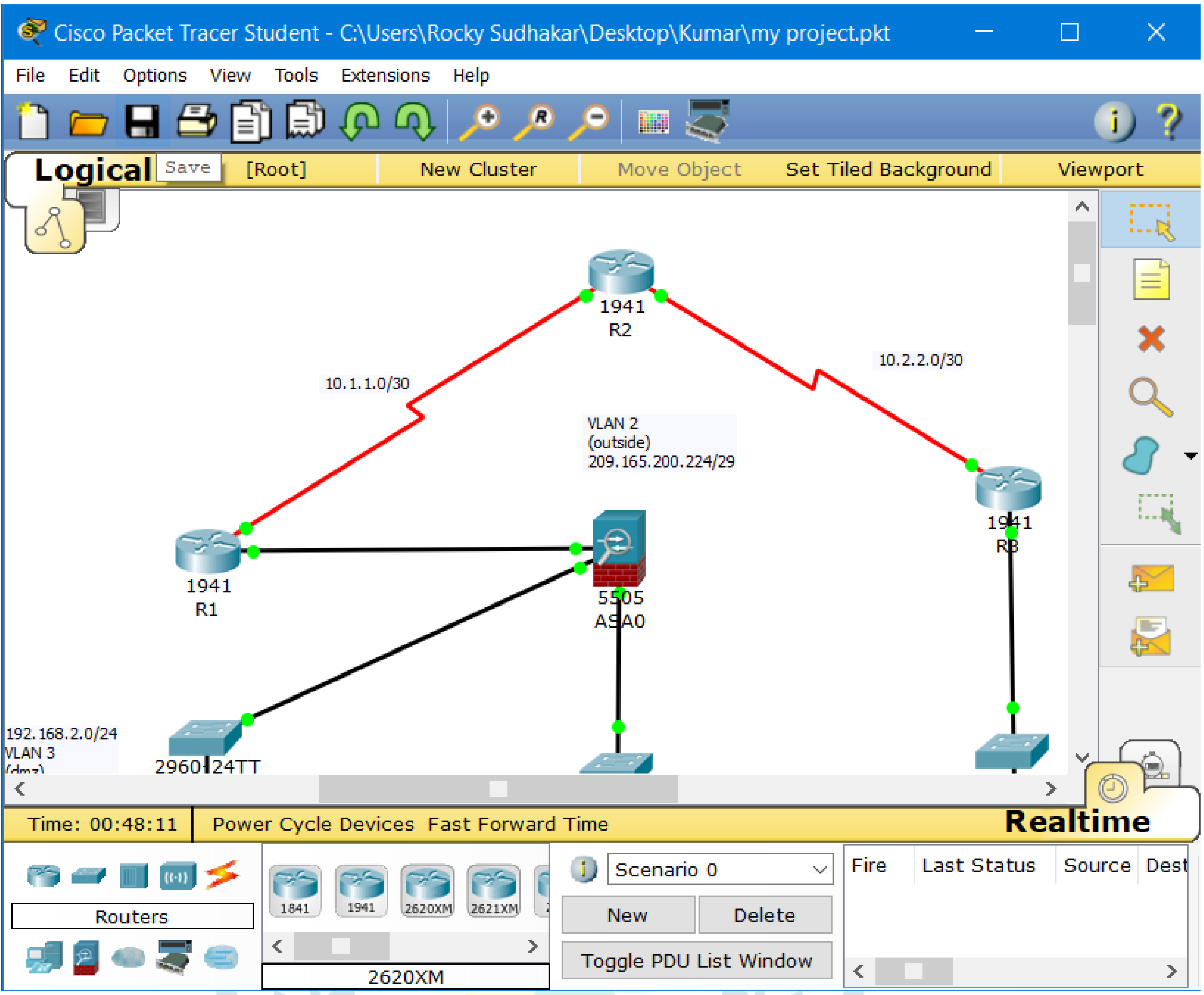


Fig 1: Nodes Representation

3.1 OBJECTIVES

- **Verify connectivity and explore the ASA**
- **Configure basic ASA settings and interface security levels using CLI**
- **Configure routing, address translation, and inspection policy using CLI**
- **Configure DHCP, AAA, and SSH**
- **Verify the connectivity of the SSH connection and make sure the connection is secure.**
- **Configure a DMZ, Static NAT, and ACLs**

4.PROCESS OF IMPLEMENTATION

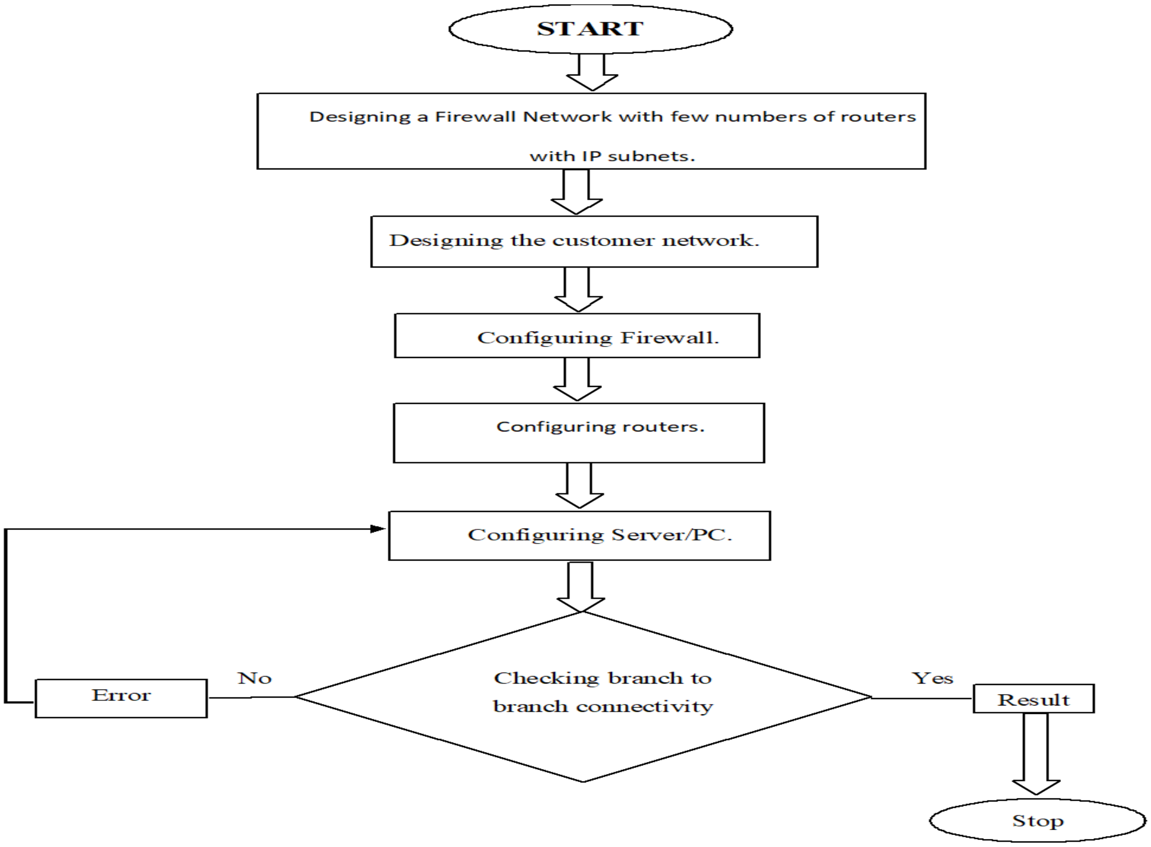

START
Designing a Firewall Network with few numbers of routers with IP subnets.
Designing the customer network.
Configuring Firewall.
Configuring routers.
Configuring Server/PC.
Checking branch to branch connectivity
No
Error
Yes
Result
Stop

Fig 2: Flowchart Representation

4. EXISTING SYSTEM

It is used to protect networks or network devices, such as industrial PCs, control systems, cameras, etc., from unauthorized access by preventing network traffic to or from the systems. The first broad distinction here is the difference between host firewalls and network firewalls.

The first is installed on a computer (host) or already provided by the operating system, as a software feature. Examples of these firewalls are the Microsoft Windows system firewall or the IP table firewall provided with most Linux systems. Network or hardware, firewalls are important elements in industrial facilities, especially when they are connected to additional networks or when wire transmissions are combined with less secure network technologies (e.g. wireless networks).

Demerits

1.) a firewall at the boundary of a network can thus, for example, include rules in the form of "A communication link within the the network can only take place with a specified server" or "Only the PCs for remote maintenance can be reached outside the network, not any other devices‖.

2.) creating special rules, such as for industrial protocols is also possible.

5. PROPOSED SYSTEM

Communication from wireless to wired networks should also be controlled by firewalls. For example, the communication of a tablet, which is connected to a device via a WLAN, can be limited so that it can only access data through the user interface, but not additional subsystems or other devices connected to it. If a client is integrated into a WLAN, it is possible, in principle, to communicate directly with all other devices in the same (sub)network. Thus, an attacker can extend a successful attack on a client that is connected to the WLAN to any other device on the Ethernet network. This problem can be solved by restricting the forwarding of messages between WLAN clients with a firewall at the WLAN access point. Here, too, there is a need for a transparent layer 2firewall which can filter communication within a network (directly between the WLAN devices in a network). In order to do this, the firewall must be implemented directly at the access point. Industrially hardened devices are important here as well. In such cases, high-quality network switches can also use less powerful stateless filtering rules. These rules are usually not referred to as firewall rules, rather as access control lists (ACL). ACLs are suited for any situation where rapid filtering must take place within a network.

Merits

1.) firewalls play various roles in the partitioning of network portions. For one, a firewall can protect a company against threats from the outside.

2.) in many cases, this overall protection is the domain of IT firewall solutions, which are placed in a company‘s data center.

3.) on the other hand, they can also be implemented, for instance, in production in order to effectively separate the production network from the rest of the company network.

6.NETWORK TOPOLOGY

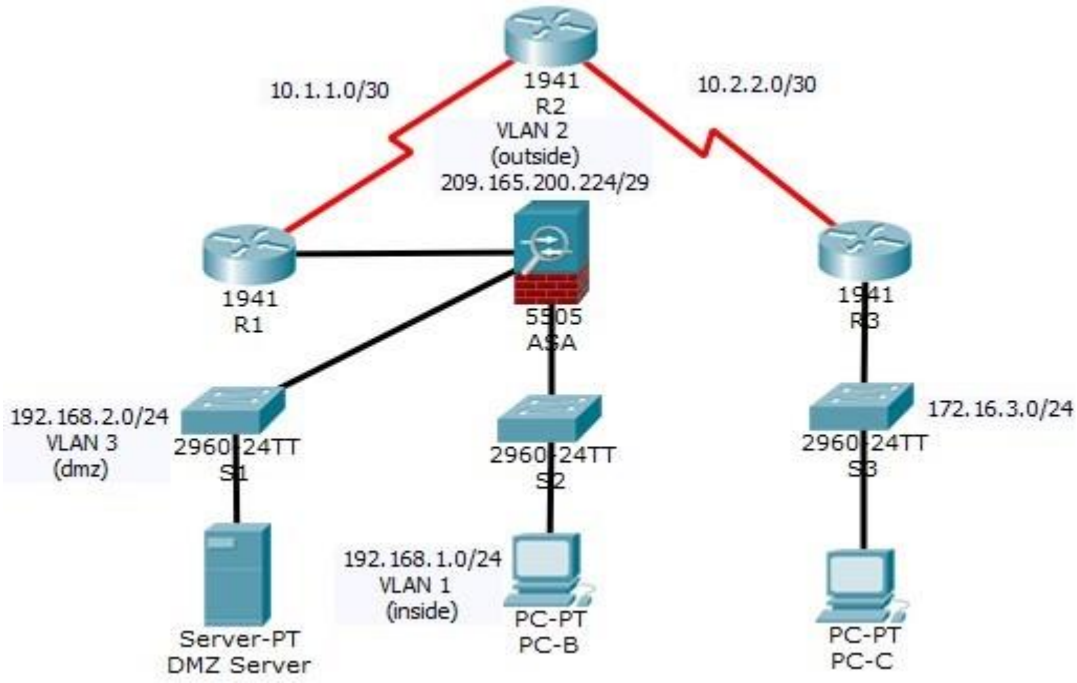
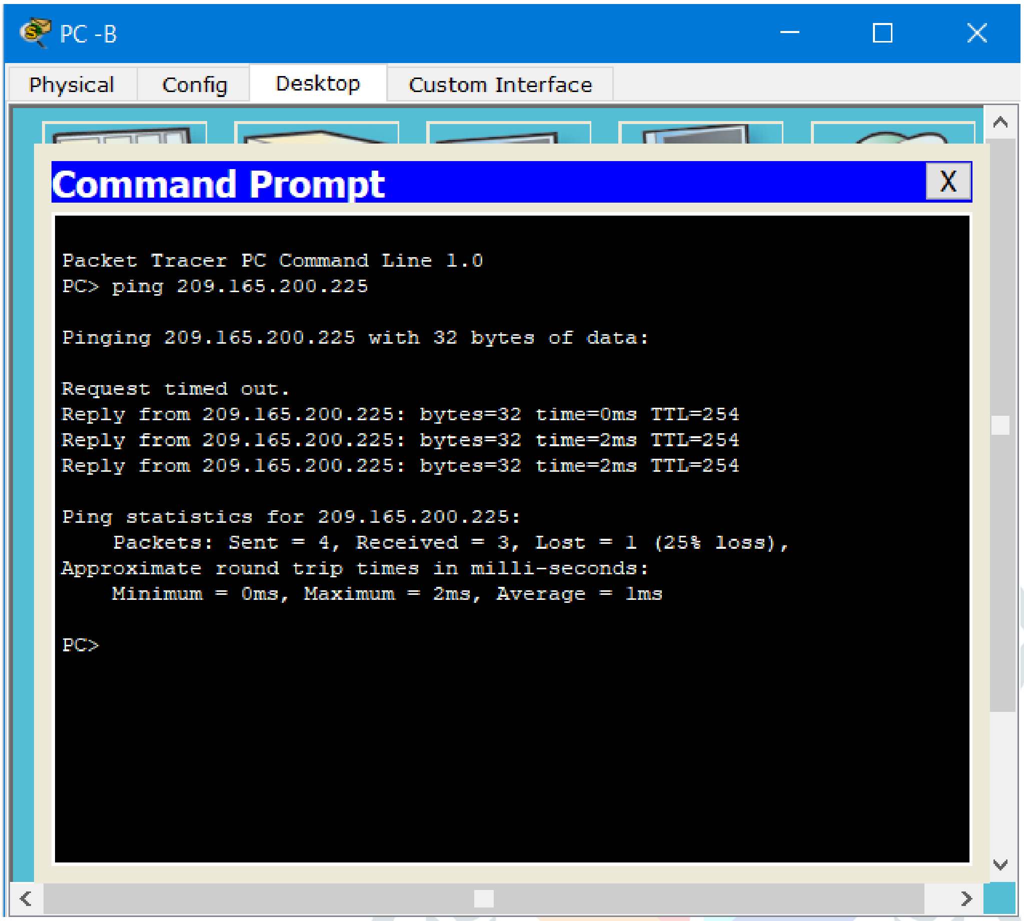


Fig 1: Network Topology

7. RESULT



```
Packet Tracer PC Command Line 1.0
PC> ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Request timed out.
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Reply from 209.165.200.225: bytes=32 time=2ms TTL=254
Reply from 209.165.200.225: bytes=32 time=2ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms

PC>
```

8. CONCLUSION

It is clear that there is a need for security in private networks connected to the Internet. To maintain security in networks, we must have to implement firewall as we can protect our devices connected through the Internet. With this, we realize the potential of firewall implementation and its various applications in a situation which can be utilized to produce the desired effect. We learn about the effectiveness of having a firewall which can constantly filter out the undesired parts of the communication packets provided by the source site. A firewall is an important and necessary part of that security, but cannot be expected to perform all the required security functions, but performs adequately.

9. REFERENCES

[1] Firewall by Dr. TalalAlkharobi.

[2] Website - www.cisco.com

[3] Network Security First –Step: Firewalls- Donald Stoddard, Thomas M