SSRG International Journal of Electronics and Communication Engineering Volume 7 Issue 4, 14-20, April 2020
ISSN: 2348 – 8549 /doi:10.14445/23488549/IJECE-V7I4P104 © 2020 Seventh Sense Research Group®

Implementing Secured Network for Tier 1 Organization

Ms. Siddhi Narendra Jadhav[1], Ms. Suruchi Sandip Shinde[2], Ms. Harshada Ramchandra Yedve[3], Mrs.S.V.Chougule [4]

Department of Electronics & Telecommunication Engineering, Finolex Academy of Management & Technology, Mumbai University, Ratnagiri
P- 60¸ P- 60/1, MIDC, Mirjole Block, postal code -415639,Ratnagiri,Maharashtra,India.

Received Date: 15 March 2020
Revised Date: 21 April 2020
Accepted Date: 25 April 2020

Abstract
In today's internet and data communication, security is a major concern to protect confidential data, privacy policies, and many more. Data integrity, confidentiality, and authenticity of sensitive information have become important aspects for organizations. While no network is immune to attacks, a stable and efficient network security system is essential to protecting organization data. A good network security system helps businesses reduce the risk of falling victim to data theft and sabotage. Attacks made on a network or wirelessly cannot be identified directly, so they are generally known as major attacks and harmful attacks. This paper discusses network security aspects of Tier-I organization and implementation of the same using two-stage firewalls. Two firewalls are implemented so that one is between a private network and a Demilitarized zone, and the other is between a demilitarized zone internet service provider. The network becomes perfectly secured so that if an attacker cracks firewall 1, it can stop at firewall 2; it is some filtration of unwanted things in the network.

Keywords — *Firewall, Internet Service Provider, Demilitarized zone, private network.*

I. INTRODUCTION

In today's internet and data communication, security is a major concern to protect confidential data, privacy policies, and many more. Data integrity, confidentiality, and authenticity of sensitive information have become important aspects for organizations. While no network is immune to attacks, a stable and efficient network security system is essential to protecting organization data. In this paper, we are going to secure the network of tier 1 organizations. This paper discusses network security aspects of Tier-I organization and implementation of the same using two-stage firewalls. Two firewalls are implemented so that one is between a private network and a Demilitarized zone, and the other is between a demilitarized zone internet service provider. By doing so, the network becomes perfectly secured so that if an attacker cracks firewall 1 it can stop at firewall 2, it is some filtration of unwanted things in the network.

The security of any network plays a strategic role in the modern computer system. Different types of attacks directly attack the system for hacking or data corruption purposes. Unauthorized access, Active eavesdropping, Man in the Middle Attack, Denial of Service are some most harmful and widely used attacks in wired and wireless networks.

Tier1 companies are the suppliers of Original Equipment Manufacturer (OEM) Components to the parent company/industry that manufactures bigger products using smaller components. Tier 2 companies are the key suppliers to tier 1 company, without supplying a product directly to OEM companies. Tier 1 companies are typically the largest company in a supply line. They often supply the most critical piece of the manufacturer's product. Tiered supply chains are often used when a final product requires many parts, such as the automobile and computer industries. Some tier-one companies provide manufacturing services to allow the original manufacturer to assemble, sell, and market products without producing pieces themselves. To enforce high protection levels against malicious attacks, several software tools have been currently developed. GNS 3 software plays an important role in security purposes. In this paper, security is done by using a firewall in GNS 3 software.

II. LITERATURE SURVEY

Most of the time, organizations focused more on the wireless side of the network. When it comes to security, because Wi-Fi has no physical fences, after all, a war-driver can detect their SSID and launch an attack while sitting out in the parking lot. Nevertheless, in a world of insider threats, targeted attacks from outside, and hackers who use social engineering to gain physical access to corporate networks, the security of the network's wired portion should also be a major concern.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Most of the devices on the existing networks are left with default settings or configured with Joe credentials. The maximum part of the running configuration is left untouched and works with the default settings and configurations, leading to a system compromise of known vulnerabilities or bugs.

With the advent of the internet, security became a major concern, and the history of security allows a better understanding of the emergence of security technology.

The literature survey regarding network security in various domains is discussed below: Computer networks have become increasingly ubiquitous. The world has come to rely on these networks to provide transport for many different mission-critical services. However, with the increase in network applications, there has also been an increase in difficult network administrators and different types of attacks.

Designing educational resources allow students to modify their learning process. In particular, Online and downloadable educational resources have been used in engineering education. Usually, these resources are free and accessible from the web. Besides, they are design and developed, and lectures and used by their students. However, students are rarely developed by students to use by other students, i.e., LAN and MAN. This paper has presented an assessment in a computer network's virtual laboratory with free stimulation tools such as GNS3. [1]

Today, every business in this world, regardless of its size or type, believes that internet access is crucial if they want to compete effectively. The need for Network Security is accelerating at the same pace as that of increased Internet usage. A firewall is a hardware device or software system or group of systems (router, proxy, or gateway) designed to permit or deny network transmission based upon a set of security rules and regulations to enforce control between two networks to protect "inside" network from "outside" network. A firewall could also be a hardware device or a software program running on a secured host computer, as stated above. A firewall inspects all the traffic between the two networks and checks that they meet all the prettified prototypes and protocols. A firewall is routed between that networks only if they follow the prettified prototype; else, if they do not follow the prototype, they are stopped. A firewall helps limit unwanted or malicious hosts or users' entry and helps in dismaying with all the upcoming threats.

A firewall is a mechanism to enforce a network domain security policy by using a policy Language, a policy distribution scheme enabling policy control from a central point, and certificates, enabling the identification of any member of the network policy domain. It secures the network by protecting critical network endpoints, exactly where hackers want to penetrate. It filters traffic from both the internet and the internal network. They provide unlimited scalability, and also overcome the single point of failure problem presented by the perimeter firewall. [2]

The security of computer networks plays an important role in modern computer systems. Many software tools have been currently developed to stop high protection levels against malicious attacks [3]. The malicious attack creates problems in any network. Network security consists of policies and provisions.

Approve by the network administrator to avert or monitor unauthorized access, misuse, or modification in the system. Network security includes authorization access to data in a network and which is controlled by the network admin. It has become important to personal computer users and organizations. Network security is becoming more important because of intellectual property that can be easily obtained through the internet. [4]

The three primary goals of network security are confidentiality, integrity, and availability by using a firewall. A firewall is used to provide security by applying security policy. The policy is a list of rules which define an action to perform on matching packets. Firewall can also perform functions like gateway antivirus. [5]

Managing information security risk is an essential element of the organization of the overall Risk management process. Tier 1, organizational level, addresses risk by establishing and implementing Governance structures consistent with the strategic goals and objectives of Organizations. Governance structures Provide oversight for organizations' risk management activities and include establishing and implementing a risk executive (function). The Establishment of the organization's risk management strategy, including the determination of risk tolerance and the development and execution of organization-wide investment Strategies for information resources and information security. [6]

Tier1 organization is related to Tier 1 Company. Tier 1 has its unique characteristics, follows its particular accumulation strategies, and distinguishes itself in its organizational Capacities. Tier 1 companies Occupy in the organization of global production networks and develop counter-strategies Tailored specifically to this type of company. The Overall work related to Tier1 Company is done in Tier1 organization. [7]

In any organization, integrity, confidentiality, and availability are important factors to make organization data secure. The information security maturity model (ISMM) is a model to evaluate organizations' ability while attacks. This model defines a process that manages, measures, and controls all aspects of security. It relies on four core indicators comprising of different compliance states for benchmarking and as an aid to understanding the security needs in the organization. The study's core objective is to develop a model that would help universities determine the level of maturity regarding information security. [8]

An enterprise's important task is decision-making, which involves risk management to be carried out regularly. Electronic information, which can be termed as an information asset, needs to be secured and protected against malicious attacks. This project's main motto is to reduce the risks and manage the uncertainties to improve its performance. [9]

III. METHODOLOGY

The implementation of a secured network for tier 1 organizations is done by using GNS3 software. GNS3 software allows many components at a time; also, it is open-source software, so it is more preferred in this topology. It consists of two firewalls that secure the network perfectly and surely. The idea for each method, specification, design, and implementation is described in section IV.

IV. IMPLEMENTATION

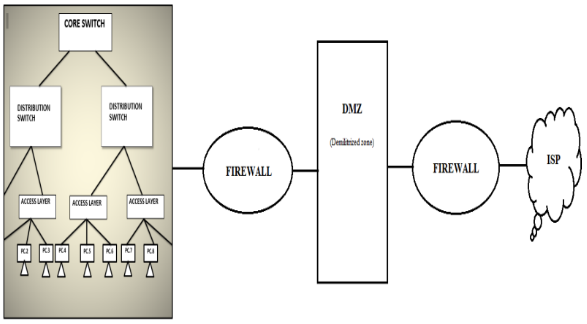


Fig 1: Diagrammatic representations of Network topology

A. Secured network consists of three basic layers are as follows:

1. Access layer
2. Distribution layer
3. Core layer

1. Access layer –

The access layer is consisting of an access switch and end devices. In this layer, end devices like printers, scanners, pc are connected to the access switch. They are connected via copper cables as it requires less energy, current, and less data is required, i.e., 100MB.

2. Distribution layer-

The distribution layer consists of a distribution switch where the access layer switch is connected. Here speed requires is a little bit more, i.e., 9.6Gbps. In this layer, the number of switches is less than the access layer.

3. Core layer-

The core layer consists of a distribution switch where the distribution layer switch is connected. As the network's speed changes, layer by layer core layer requires more speed of the network. So instead of copper cable, fiber cables are usually referred to, and in this layer, more data is required. This layer is the last and connected to the firewall from which part of security begins.

B. Firewall

A firewall is a device that allows multiple networks to communicate with one another according to a defined security policy. A firewall is a system that enforces an access control policy between two networks—such as your private LAN and the unsafe, public internet. [10] They are used based on the need for networks of varying trust levels to communicate with one another. For example, a firewall typically exists between a corporate network and a public network like the internet. It can also be used inside a private network to limit access to different parts of the network. Wherever there are different levels of trust among the different parts of a network, a firewall can and should be used. Firewalls are similar to routers in that they connect networks. A firewall can be either hardware-based or host-based. A hardware-based firewall usually means specialized network boxes, such as routers or switches, hardware-based firewall; a host-based firewall is easier to use for individuals or small organizations.

C. DMZ (Demilitarized Zone)

In computer security demilitarized zone is a physical subnetwork that accommodates and displays an organization's external services to a mistrusted network, generally a larger network such as the internet. The purpose of a DMZ is to add a layer of security to an organization's local area network, and hence hacker cannot access any network using the internet; because of this, DMZ is also called perimeter networks.DMZ provides security without the accessibility of data [11]. Dmz function is small and is located between the internet network and private network. The Dmz function is similar to a firewall and is used for security purposes. Dmz is an area of the network where you can place your email server, FTP server, and web server that you want available for the public to used or access. Companies use DMZ for websites that organize certain services and information for clients. If the webserver on your DMZ is compromised, the attacker can influence what is inside the DMZ and not the internal local area network protected by a firewall. Router and switch provide the connectivity within the demilitarized zone and the other network connected to Dmz. The switch provides many features, including port security.

D. ISP

ISP stands for Internet Service Provider. ISP is a company that provides internet and similar services such as Website designing and virtual hosting. For example, when you connect to the internet, the connection between your Internet-enabled device and the internet is executed through a specific transmission technology that involves transferring information packets through an Internet Protocol route. Data is transmitted through different technologies, including cable modem, dial-up, DSL, high-speed interconnects. ISPs in Malaysia should improve their service reliability and improve their overall service offerings. All networking companies and relevant agencies need to continue providing the needed knowledge and communication infrastructure required to make government agencies and industries work effectively in delivering services to customers. [12]

V. DESIGN DETAILS

Network Topology is an arrangement of a communication network element such as nodes, switches, routers, and network connections.

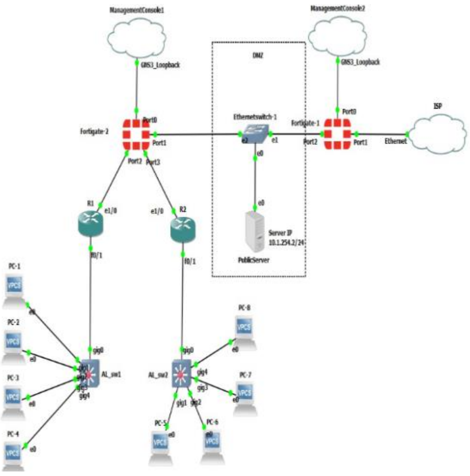


Fig 2: Network Topology

This paper gives an idea about implementing a secured network for tier1 organizations. In this paper, security is the major aspect, so that GNS3 software is used and implemented the topology because as compared to other software GNS3 supports multivendor, scaling, it can connect to the real world is open source implemented the topology.

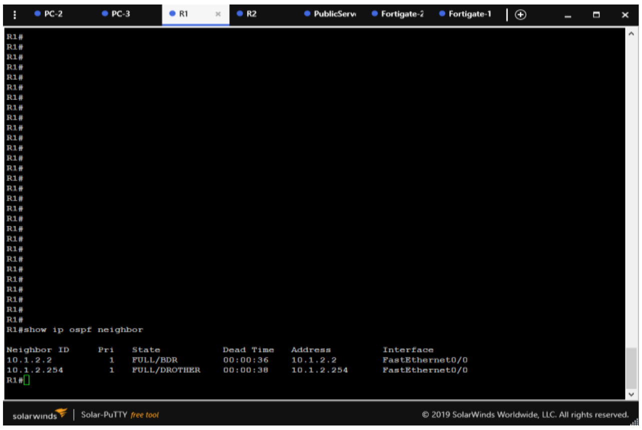
After installing software and components, files in the software implementation of topology started. First of all, the topology is divided into three major parts those are private network, demilitarized zone, internet service provider.

The private network consists of routers, PCs, switches, so using curser drag and drops process done and connecting all router, PCs, switches as per the topology. By using solar putti, all configurations are done on the components. In brief, First start from the base, which is the PCs. So, connect the PCs to switch1 and switch2, i.e., sw1 and sw2. Configured PCs are namely pc-1, pc-2, pc-3, and pc-8. It is also known as VPC's in solar putty, i.e., Virtual PC. PC has its IP address that is given during configuration in command prompt. The main router has two ports which are ports 1/0 and 0/1. In these two ports, Port 1/0 is connected to the 1st firewall, i.e., FortiGate-2. The firewall has four ports, i.e., port0, port1, port2, and port3. For this configuration, port0 is connected to the cloud, i.e., management console1. Port2 and port3 are connected to router1 and router2. Moreover, the last port1 is connected to the switch, which is the part of DMZ, i.e., Demilitarized zone, firewall is used for security purposes.

After implementing a private network, a demilitarized zone is implemented to add a firewall and public server. A demilitarized zone is an additional function of security. For this configuration, we used one switch & one public server. The public server has its IP address that is given in the command prompt during configuration. After this, one more firewall is used, named Fortigate-1; this firewall has the same configuration as the first firewall. Finally, the second firewall is connected to the ISP, i.e., the internet service provider.

The last one is ISP, which is an internet service provider attached to the demilitarized zone. This is the outer layer of the network. The ISP provides an internet connection to the network. We can ping any pc or router to ISP, but we cannot ping in a reverse manner. Also, two firewalls help us with extra security.

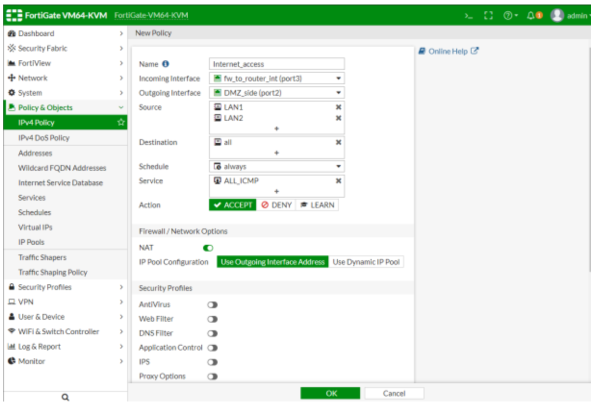
VI. RESULTS



```
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.2.2          1   FULL/BDR        00:00:36    10.1.2.2        FastEthernet0/0
10.1.2.254        1   FULL/DROTHER    00:00:38    10.1.2.254      FastEthernet0/0
R1#
```

Fig 3: OSPF protocol is run in firewall and cisco routers

Router OSPF neighborship with firewall OSPF protocol is run in firewall and cisco routers.fig1 shows the neighbor table. In this fig1, two IP addresses are there. In which 10.1.2.2 is for R2 means router2 and 10.1.2.254 is for the firewall.



New Policy

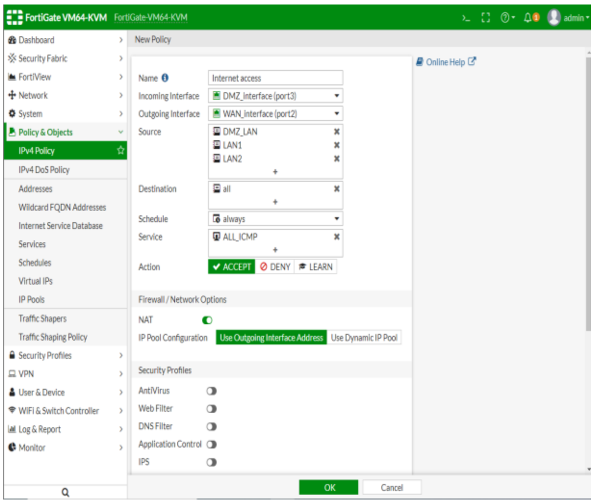
Name: Internet_access
Incoming Interface: fw_to_router_int (port3)
Outgoing Interface: DMZ_side (port2)
Source: LAN1, LAN2
Destination: all
Schedule: always
Service: ALL_ICMP
Action: ✓ ACCEPT | DENY | LEARN

Firewall / Network Options
NAT: ●
IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Security Profiles
AntiVirus ○
Web Filter ○
DNS Filter ○
Application Control ○
IPS ○
Proxy Options ○

Fig4: FW2 Internet access

Internet access policy is provided at FortiGate 2 in communication is allowed in LAN1 and LAN2 precisely. If an attacker used IPs other than LAN1 and LAN2, then there will be no communication.



New Policy

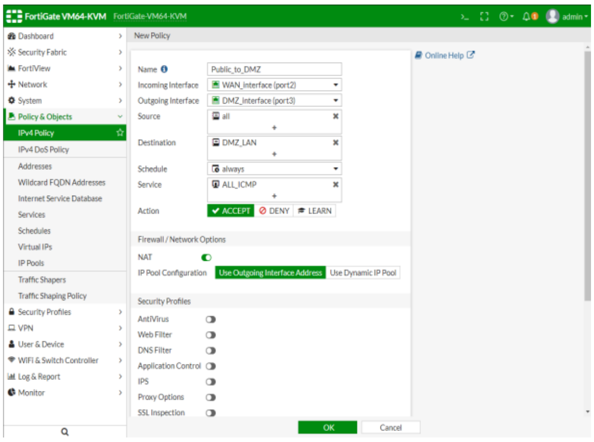
Name: Internet access
Incoming Interface: DMZ_Interface (port3)
Outgoing Interface: WAN_interface (port2)
Source: DMZ_LAN, LAN1, LAN2
Destination: all
Schedule: always
Service: ALL_ICMP
Action: ✓ ACCEPT | DENY | LEARN

Firewall / Network Options
NAT: ●
IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Security Profiles
AntiVirus ○
Web Filter ○
DNS Filter ○
Application Control ○
IPS ○

Fig 5: FW1 internet access

There is one policy written on the firewall for internet access. In which only LAN1, LAN2, and DMZ_LAN can communicate over the internet.



New Policy

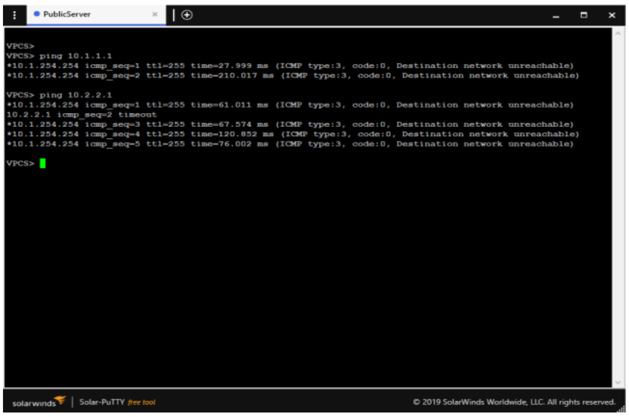
Name: Public_to_DMZ
Incoming Interface: WAN_interface (port2)
Outgoing Interface: DMZ_interface (port3)
Source: all
Destination: DMZ_LAN
Schedule: always
Service: ALL_ICMP
Action: ✓ ACCEPT | DENY | LEARN

Firewall / Network Options
NAT: ●
IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Security Profiles
AntiVirus ○
Web Filter ○
DNS Filter ○
Application Control ○
IPS ○
Proxy Options ○
SSL Inspection ○

Fig 6: FW1 DMZ access to the public network

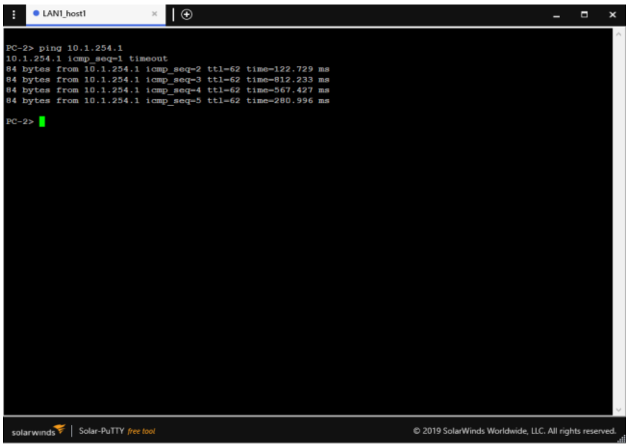
People can access only the public server through the internet.



```
VPCS>
VPCS> ping 10.1.1.1
*10.1.254.254 icmp_seq=1 ttl=255 time=27.999 ms (ICMP type:3, code:0, Destination network unreachable)
*10.1.254.254 icmp_seq=2 ttl=255 time=210.017 ms (ICMP type:3, code:0, Destination network unreachable)

VPCS> ping 10.2.2.1
*10.1.254.254 icmp_seq=1 ttl=255 time=61.011 ms (ICMP type:3, code:0, Destination network unreachable)
10.2.2.1 icmp_seq=2 timeout
*10.1.254.254 icmp_seq=3 ttl=255 time=67.574 ms (ICMP type:3, code:0, Destination network unreachable)
*10.1.254.254 icmp_seq=4 ttl=255 time=120.852 ms (ICMP type:3, code:0, Destination network unreachable)
*10.1.254.254 icmp_seq=5 ttl=255 time=76.002 ms (ICMP type:3, code:0, Destination network unreachable)

VPCS>
```

Fig 7: Public server to internal LAN

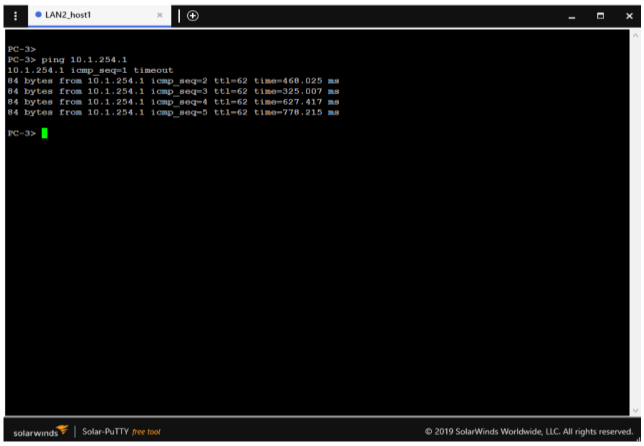
Public server to internal LAN communication is blocked.



```
PC-2> ping 10.1.254.1
10.1.254.1 icmp_seq=1 timeout
84 bytes from 10.1.254.1 icmp_seq=2 ttl=62 time=122.729 ms
84 bytes from 10.1.254.1 icmp_seq=3 ttl=62 time=812.233 ms
84 bytes from 10.1.254.1 icmp_seq=4 ttl=62 time=567.427 ms
84 bytes from 10.1.254.1 icmp_seq=5 ttl=62 time=280.996 ms

PC-2>
```

Fig 8: LAN1 to the public server

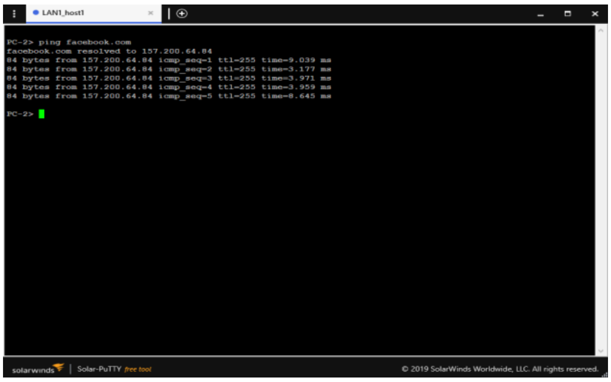
Internal LAN to public server communication is allowed.



```
PC-3>
PC-3> ping 10.1.254.1
10.1.254.1 icmp_seq=1 timeout
84 bytes from 10.1.254.1 icmp_seq=2 ttl=62 time=468.025 ms
84 bytes from 10.1.254.1 icmp_seq=3 ttl=62 time=325.007 ms
84 bytes from 10.1.254.1 icmp_seq=4 ttl=62 time=627.417 ms
84 bytes from 10.1.254.1 icmp_seq=5 ttl=62 time=778.215 ms

PC-3>
```

Fig 9: LAN2 to the public server

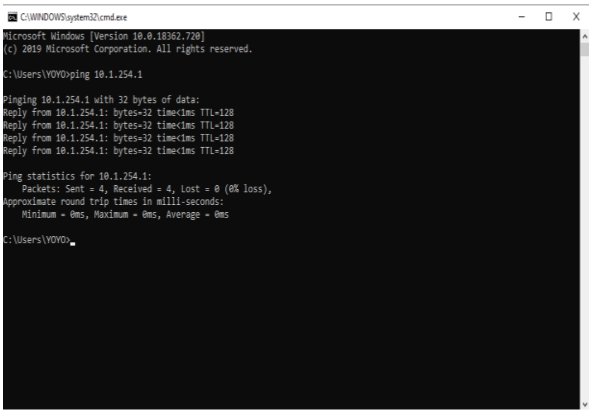
Internal LAN to public server communication is allowed.


LAN1_host1
solarwinds | Solar-PuTTY free tool
© 2019 SolarWinds Worldwide, LLC. All rights reserved.

```
PC-2> ping facebook.com
facebook.com resolved to 157.200.64.84
84 bytes from 157.200.64.84 icmp_seq=1 ttl=255 time=9.039 ms
84 bytes from 157.200.64.84 icmp_seq=2 ttl=255 time=3.177 ms
84 bytes from 157.200.64.84 icmp_seq=3 ttl=255 time=3.971 ms
84 bytes from 157.200.64.84 icmp_seq=4 ttl=255 time=3.959 ms
84 bytes from 157.200.64.84 icmp_seq=5 ttl=255 time=8.645 ms

PC-2>
```

Fig 10: LAN1 to the public network

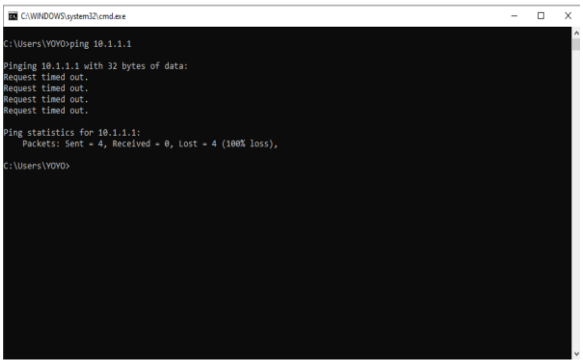
Internal LAN to internet communication is allowed; that is why we can ping facebook.



```
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\YOYO>ping 10.1.254.1

Pinging 10.1.254.1 with 32 bytes of data:
Reply from 10.1.254.1: bytes=32 time<1ms TTL=128
Reply from 10.1.254.1: bytes=32 time<1ms TTL=128
Reply from 10.1.254.1: bytes=32 time<1ms TTL=128
Reply from 10.1.254.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.254.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\YOYO>
```

Fig 11: Internet to the public server

Through the internet, people can access public services.



```
C:\Users\YOYO>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\YOYO>
```

Fig 12: Internet to internal LAN

Through the internet, people cannot access internal LAN access.

VII. SCOPE

Since India is emerging as a digital India, every industry needs to have strong data security mechanisms. The network security engineers play a vital role in operating and handling the security appliances such as firewalls and IPS to secure the organization's important data.

Network security consists of the provisions and policies embraced by a network administrator to preclude and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which the network administrator controls.

VIII. CONCLUSION

In this work, the methodology of implementing a secured network for tier 1 organization is by use of GNS3 software...the topology consists of two firewalls by which topology becomes more secured. Some limitations are also there for this network, like changing the router default password, enabling a firewall on the router. However, those limitations are not major as compare to the use of the topology. We conclude that networking topologies is of more importance than computer networking design, which is best for organization or business and advantageous for future networking systems.

IX. ACKNOWLEDGEMENT

The work is supported by TELENETWORK TECHNOLOGIES PVT LTD, Vashi, Mumbai.

X. REFERENCES

[1] Pablo Gil, Member IEEE, Gabriel J. Garcia, Angel Delgado, Rosa M. Medina, Antonio Calderon, Patricia Marti Computer Science Research Institute University of Alicante San Vicente del Raspeig "*Computer Networks Virtualization with GNS3*," Vol 22, No July 2017.

[2] Aakanksha Chopra Assistant Professor (IT), "*Security Issues of Firewall*," International Journal of P2P Network Trends and Technology (IJPTT) – Volume 6 Issue 1 January to February 2016.

[3] Rahul Pareek, Journal Of Global Research In Computer Science. "*Network Security: An Approach towards Secure Computing,*" Volume 2, No. 7, July 2011

[4] Mohan V. Pawar1, Maharashtra, "*Network Security and Types of Attacks in Network*," International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014) Procedia Computer Science 48 (2015) 503 – 506.

[5] Ramy K. Khalil, IJCSNS International Journal of Computer Science and Network Security, "*A Study of Network Security Systems*," VOL.10 No.6, June 2010.

[6] Shirley Radack "*Managing Information Security Risk: Organization, Mission and Information System View*," Volume 7, No 5, April 2016.

[7] Jeroen Merk, Merk, J. (2014) "*The Rise of Tier 1 Firms in the Global Garment Industry: Challenges for Labour Rights Advocates*," Oxford Development Studies, vol. 42 (2) pp. 277-295.

[8] Daniel Makupi, Nelson Masese, "*Determining Information Security Maturity Level of an organization based on ISO 27001*" SSRG International Journal of Computer Science and Engineering 6.7 (2019): 5-11.

[9] Mrs. V.Usha Bala, Dr.B.D.C.N.Prasad, "*Steering the Enterprise's Information System Security Risks in Relation with Uncertainty (Information System, Risks*)" SSRG International Journal of Computer Science and Engineering 5.2 (2018): 5-8.

[10] Binh Nguyen "Network Security and Firewall," A Linux Open Source Firewall Helsinki Metropolia University of Applied Science Bachelor of Engineering Information Technology Bachelor'sThesis Date 29 April 2016.

[11] Sourabh Shrimali M.Tech (Network Management & Information Security) School of Computer Science & IT Devi Ahilya Vishwavidyalaya, Indore, India "*Demilitarized Zone: Network Architecture for Information Security*," International Journal of Computer Applications (0975 – 8887) Volume 174 – No.5, September 2017.

[12] Uchenna Cyril "ISPs' Service Quality and Customer Satisfaction in the Southern Region of Malaysia," 19th Australian Conference on Information System Service Quality and Customer Satisfaction 3-5 Dec 2008.

[13] www.gns3.com

[14] Behrouz A. Forouzan "*TCP/IP Protocol suite Fourth Edition*."