J. Basic. Appl. Sci. Res., 1(10)1623-1632, 2011

ISSN 2090-424X
Journal of Basic and Applied Scientific Research
www.textroad.com

A Model Design of Network Security for Private and Public Data Transmission

Farhan Pervez, Ali Nawaz Khan, and Muhammad Waqas Anwar*

COMSATS Institute of Information Technology, Lahore, Pakistan
*COMSATS Institute of Information Technology, Abbottabad, Pakistan

ABSTRACT

The explosive growth of the Internet demands higher reliability and performance than what it was few years ago. Secured user authentication, authorization and access control have become the major challenges in a network system. When the issue is sending data to or receiving from an un-trusted public environment, a firewall should be the centerpiece of a security solution. As the data leaves the private and enters into a public network the threat to its security increases. It is therefore necessary to have a type of communication that is not vulnerable to attacks and have some restrictions within a network as well so that the threats of internal attacks are limited. We have implemented such a network design that could solve the queries related to secure private and public data transmission by providing complete secured and authorized transmission throughout the network and created VPNs over a shared public network that uses hashing and encryption algorithm to make a logical tunnel around the data packets. At the end we analyzed our traffic that enters and leaves the firewall device by using a well known device manager, ASDM.

KEY WORDS: Firewall, Network security, VPN (Virtual Private Network), ASDM (Adaptive Security Device Manager).

1. INTRODUCTION

In recent times, internet has evolved as a network of countless networks that are interconnected without any boundary. Therefore, network security has also became essential because any organizational network is accessible from any computer in the world and, therefore, potentially vulnerable to threats from un-identified users. When the issue is sending data to or receiving from an un-trusted environment, a firewall device should be the centerpiece of a security solution which essentially is a router or access server, or several routers or access servers, designated as buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network [1].

The focus of our work was to provide and configure a solution to the network security between any connected public network and private network using a firewall. The implementation also covered securing our traffic from inner threats. We further enhanced our model network by achieving reliable connectivity over a shared public network by creating point-to-point and remote Virtual Private Networks offering secure, reliable connectivity over a shared public network infrastructure such as the Internet. This service uses the encryption and hashing techniques to create a secured logical tunnel between the source and the destination [2].

2. NETWORK SECURITY MODEL DESCRIPTION

A. Placement of a Firewall device

When accessing information through an internetwork that consists of several connected networks, secure areas must be created. The device that separates each of these areas is known as firewall. A firewall usually has at least three interfaces that create three different networks. The three areas that are created are described as follows:

Inside: It is the trusted area of the internetwork. The devices on the Inside are on the organization's private network.

Outside: It is the un-trusted area of the internetwork. Usually it is known as the perimeter or border router end. The firewall secure the devices on the Inside and DMZ from the devices on the Outside.

***Corresponding Author:** Muhammad Waqas Anwar, *COMSATS Institute of Information Technology,Abbottabad, Pakistan*.
Email: waqas@ciit.net.pk

DMZ (Demilitarized Zone)

It is an isolated network (or networks) which are usually accessible to Outside users. The creation of such an area allows an organization to make information and services available to Outside users in a secure and controlled environment. Fig. 1 shows the three networks created by a firewall with three interfaces.

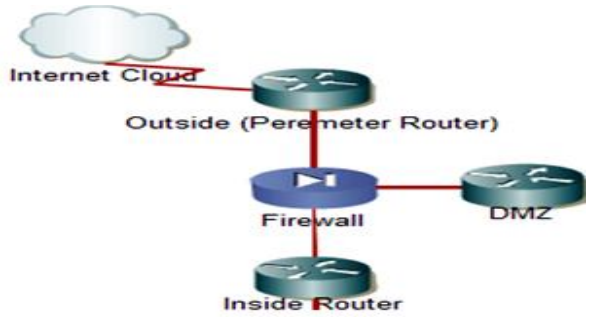


Fig. 1 General Network Design Using a Firewall

The baseline perspective for a firewall is to perform the following functions: permit no access from the Outside to the Inside; permit limited access from the Outside to the DMZ; permit all access from the Inside to the Outside; permit limited access from the Inside to the DMZ [3]. In many network designs there are exceptions to some or all of these rules. For example, all traffic is not permitted to traverse from Inside to Outside. Potentially an IP address, a subnet, or the entire inside network may be restricted from utilizing a particular application (port).

B. Point of Creation of VPN Tunnels

VPN is a secured logical tunnel, created between the source and the destination over a shared public network. This tunnel can be formed between two fixed points i.e. a fixed source and a fixed destination. It can also be created between a fixed point and a remote point i.e. a fixed source and a remote destination [4]. These two types of VPNs are called Site-to-Site VPN and Remote Access VPN (RA-VPN) and are the most commonly used VPNs in a network infrastructure.

Site-to-Site VPN

A site-to-site VPN is created between two or more routers over a public network that is shared. It secures traffic on the vast internet infrastructure or over wide area networks. It provides reliable connectivity between two or more fixed locations. Fig. 2 shows the site-to-site VPN topology.

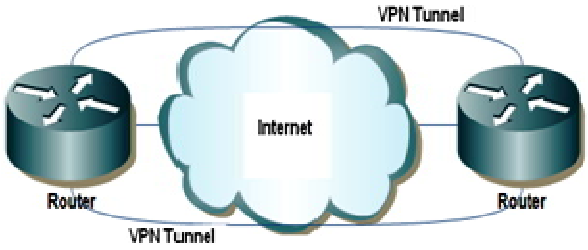


Fig. 2 Router to Router VPN Tunnel

Remote Access VPN (RA-VPN)

A remote access VPN, as the name suggests, is created over a shared public network between a fixed location and a remote location. It provides reliable connectivity between a remote user and the shared network router. Fig. 3 shows the Remote Access VPN topology.

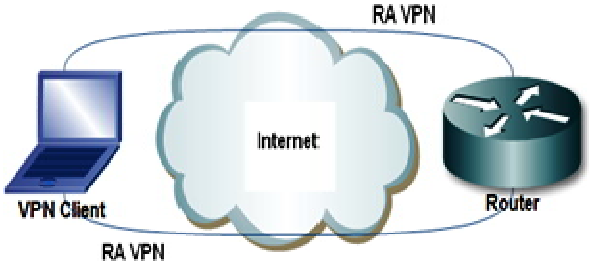


Fig. 3 Remote user to Router VPN Tunnel

C. Definitions and Descriptions

Telnet

Telnet is the standard terminal emulation protocol within the TCP/IP protocol suite defined by RFC 854. It allows users to log on to remote networks and use those resources as if they were locally connected. When securing a network, it is important to control Telnet access to the router and other networking equipment because Telnet access can lead to privileged access making it possible to change network configuration [5].

Ping

Ping is an Internet Control Message Protocol echo packet that is used to establish whether or not a remote host is reachable [6].

Access Control List

Access control lists (ACLs) filters traffic by denying or permitting the traffic or by classifying the traffic for network address translation (NAT). ACLs are used in firewalls to filter traffic. Security rules to permit or deny networks or any user are defined by access control lists (ACLs) on firewall. The firewall does not allow any traffic unless it is specified in access control lists (ACLs). Fig. 4 shows the direction in which the inbound and outbound ACLs are applied.

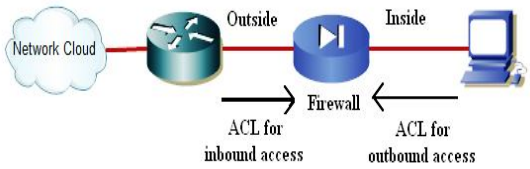


Fig. 4 ACLs for Inbound and Outbound Access

Object ACLs

Standard access control lists (ACLs) are fine for medium and small size organizations where there are only few hosts, 3 or 4 different services and few servers. But in large organizations, access control entries can increase exponentially, ACLs can have thousands of thousands of entries. Object ACLs simplifies entries and make some official control lists by using proper grouping techniques. We can actually reduce 3000 plus access control entries to just few hundreds by using these object ACLs on firewall.

Following are some of the uses of access lists in firewall.

- **Provide network security rule definition:** The rules for one security domain to access the other security domain are described using access lists.
- **Used in configuring Policy Network Address Translation (NAT):** Access lists are used to identify Policy NAT for specific source or destination IP addresses.

Policy Network Address Translation

Policy NAT enables to identify local traffic for address translation by specifying the source and destination addresses in an ACL. With policy NAT, we can create multiple policy NAT statements based on unique source-port and destination-port combination ACL statements. We can then match different mapped addresses to each source-port and destination-port pair.

Transparent Firewall

There are two modes of a firewall; router firewall mode and transparent firewall mode. The transparent firewall mode is used to secure a private network from inner threats, i.e. from layer 2 attacks. The router mode is used to secure a private network from a public one. It works on Layer 3, having multiple interfaces that may be used for Context-Based Firewalling.

Context-Based Firewall

A single firewall device can be set-up as two or more than two logical firewalls by using the multiple-context mode of it. This enables the network designer to have separate set of rules for different group of people. When we convert from single mode to multiple modes, the running configuration is converted into a new startup configuration that comprises the system configuration and Admin.cfg that contains the admin context. The original running configuration is saved as old_running.cfg [7]. Fig. 5 shows this multiple context mode concept.

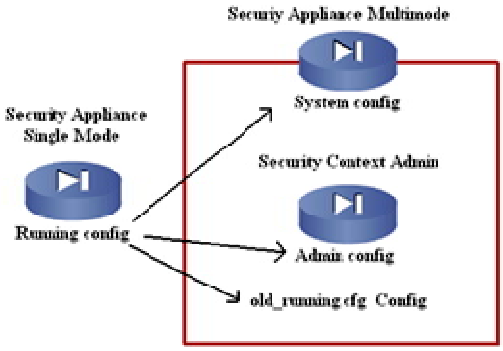


Fig. 5 Multiple Context Multimode Concept

AAA Services

Authentication, Authorization, Accounting (AAA) is used by a firewall device to identify who the user is, what the user can do, and what the user did [8]. Authentication determines a user identity and verifies the information provided by the user; most commonly authentication uses a username and a fixed password. Once the user has authenticated the authentication server may be configured to allow specific authorization based upon the user ID an password. Authorization defines what the user can do. When the user has logged in and accessing the service, or network a record of what the user is doing may be kept. Accounting is the action of keeping track of what the user does. AAA can be processed in the following manner:

- The client request access to some service, the firewall acts as a gateway between the client and the device the service is required on.
- The firewall receives the information and forwards it to the AAA server where it is confirmed to be permitted or denied. A server is defined as a logical entity that provides any of the three AAA functions.

Access control server software is an authentication server that can be configured to authenticate and authorize users by controlling access. By using it, it is possible to allow certain authenticated users to access to a network. An example is that to only allow those users from inside network through the firewall who have a valid ID and password to access the internet. It is possible to restrict authorization of that authenticated users. It is also possible by configuring the firewall and AAA server to restrict the services that can be accessed (FTP, HTTP or Telnet). Fig. 6 shows an administrator getting access to the firewall by sending authentication request to the Access server.

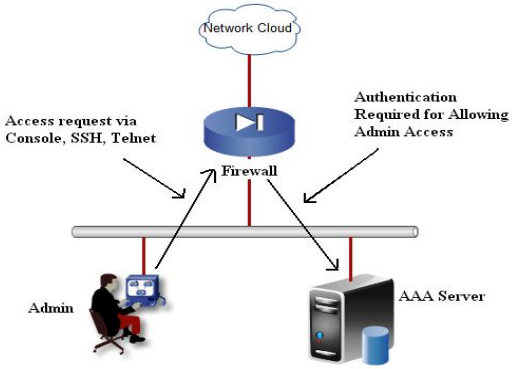


Fig. 6 Authentication Access on Firewall Through Access Control Server

3. IMPLEMENTATION AND CONFIGURATION DETAILS

Designing a Network Infrastructure

Designing a network infrastructure is one of the topics that are subject to opinion. A network should be reliable, manageable and cost effective that meets or exceeds the requirements of the project. A very important aspect of designing is to understand the features and capabilities of the hardware and software. One of the keys to success is to "keep it simple." This makes it easier to understand, configure, maintain and troubleshoot [7]. For network design, we have considered the following three-step process as we plan and implement the design:

Step1: Determine Design considerations.
Step2: Determine Deployment options.
Step3: Determining Placement

Step1--Determining Design Considerations:

In the process of the network design, first step is to determine exactly what you are attempting to accomplish and document that information. In security design a security policy is therefore imperative.

Documenting the Process

Documenting the process is one of the most important aspects of creating a network design because it provides a record of the requirements, the scope of the project, and so on. This document should be very clearly written to avoid ambiguity and will provide foundation for the entire plan. Project documentation of our work is as follows:

The End Goal

A model design of Network Security for Private and Public Data Transmission.

Resources Need to be Secured

Private network with network ID 192.168.1.0 and 10.0.0.0 to be secured from inner threats and public network's threats Publically shared network with network ID 1.0.0.0 to be secured from attacks on data during transmission using VPN Tunnel.

Applications

Transmission Control Protocol (for TELNET)
Internet Control Message Protocol (for PING)
Hypertext Transport Protocol (for WEB)

Allowing Access

Context C1

10.1.1.3 and 10.1.1.4 are allowed to ping site-to-site VPN router by using Object ACLs on Context-based Firewall
10.1.1.4 is not allowed to telnet perimeter (border) router by using Access Control Lists (ACLs) on Transparent Firewall
10.1.1.4 is allowed to telnet site-to-site VPN router with hiding the original IP address by using Policy NAT on Context-based Firewall
10.1.1.5 is allowed to ping site-to-site VPN router with hiding the original IP address by using Policy NAT on Transparent Firewall
Site-to-site VPN router is allowed to telnet 50.1.1.1 (NAT IP) which will redirect it to 10.1.1.5 by using Static Translation on Context-base Firewall
Site-to-site VPN router is allowed to telnet context base firewall C1 with port 2020 which will redirect it to 10.1.1.3 by using Static Translation

Authenticating Access

Context C2

192.168.1.3 is allowed to http site-to-site VPN router by using access control server
192.168.1.3 is allowed to telnet site-to-site VPN router by using access control server
12.1.1.2 (perimeter/border router) is allowed to ping 192.168.1.3 by static translation

Hardware Requirement

We have used two firewalls (Context based & Transparent), 2 routers, 2 switches and 2 servers.

Software Requirement

Firewall IOS (Cisco PIX/ASA version 7.2(3) and above)
Access Control Server (Cisco-ACS)
VPN Client Software (Cisco-VPN-CS)
Adaptive Security Device Manager (ASDM)

Multiple Contexts

Multiple contexts are very useful for us because we have routed and transparent firewalls in our topology and we have supported multiple customers with different security policies.

Creating VPN

For hashing, the algorithm which we are using is **"md5"**
For encryption, the algorithm which we are using is **"des"**

Step 2--Determining Deployment Options

After compiling the documentation of the design considerations, in Step2 we determine the deployment options. This would help us out to set up our firewall device for the final design topology and would enable us to decide which type of VPNs to create. The following are some points that need to be well cleared in our mind before implementing the final hardware:

Should the firewall be in single-context mode? : If a single organization maintains control over the firewall and logical separation of multiple firewalls is not required, the answer could be yes.

Should the firewall be in multi-context mode? : If there are multiple organizations, or separation of applications/services is required, multi-context mode may be a good solution.
Note: According to our requirements we would therefore be using the multi-context mode of the firewall at the perimeter router end and a single-context mode firewall in the internal network.
Should the firewall be configured in router mode? : Router mode is a great solution if a need exists for multiple interfaces. For example, you may require inside, outside and DMZ interfaces, which are possible only in router mode.
Should the firewall be configured in transparent mode? : Transparent mode can be a solution if a need exists for securing from Layer2 attacks. Transparent mode supports only two interfaces and no IP addressing is required.
Note: According to our requirements we would therefore be using router mode with multiple contexts at the perimeter router end and transparent mode with single context in the internal network.
How are access-lists created? : Based on the information gathered for who needs access, the best option is to create a very limited rule set to allow only specific traffic through. Then use noise level detection (users complaining about not being able to access the service) and modify the access list accordingly.
Should the site-to-site VPN tunnel be created? : Site-to-site VPN tunnel is a great solution when you want to secure your data which is passing over public network between two fixed locations.
Should the remote access VPN tunnel be created? : Remote access VPN tunnel is a great solution when you want to communicate over public network between remote locations where IP address of host network is not stationary.
Note: According to our requirements we would therefore be using both site-to-site and remote access VPNs at the perimeter router end.

Step 3-- Determining Placement

The next step is to determine where or how to logically place the firewall and create VPNs. Our implementation consists of three phases:
Securing Private network from inner threats
Securing Private network from Public one
Securing communication at shared Public network

Securing Private Network from Inner Threats

We would place a transparent firewall inside a network and use it as Layer 2 bridge between two switches. The firewall device would be configured as a single-context device in the transparent mode with just two interfaces. This would prevent any specific user to have unauthorized access to any other internal network user. The idea of such placement of firewall is shown below in fig. 7:

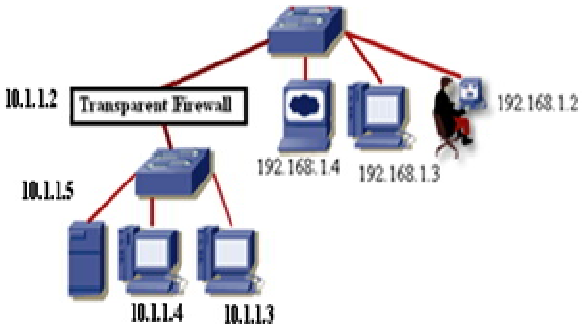


Fig. 7 Securing Inner Threats

Securing Private Network from Public One

We would place a firewall at the perimeter router end. It would be configured as a multiple-context device in the router mode. The firewall acts as a Layer 3 entity in this mode, which can queue up the packets at its input, process them according to the rule-set and route them forward to their specified destination. The idea of such placement of the firewall is shown below in fig. 8.

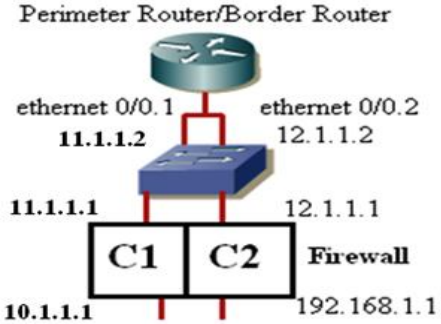


Fig. 8 Securing Private Network

Securing Communication at Shared Public Network

We would create VPN tunnels on shared public network. This would enable secured connectivity on an unsecured network path. Both site-to-site and remote access would be implemented so as to fully support our final design with all strategies of security. The idea of such tunnels is shown below in fig. 9.

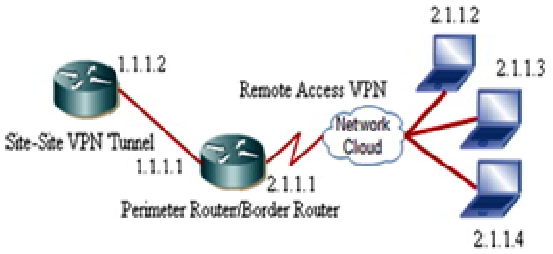


Fig. 9 VPN Tunnels

Final Design

The section shows the final design implemented on the hardware devices. This topology is designed to fully cover all the aspects discussed so far. The implementation is based on to secure private network from a public one and to secure this private network from inner threats also. VPN tunnels are also created that are to achieve reliable connectivity over shared public network. Fig. 10 shows the final design topology diagram implemented.

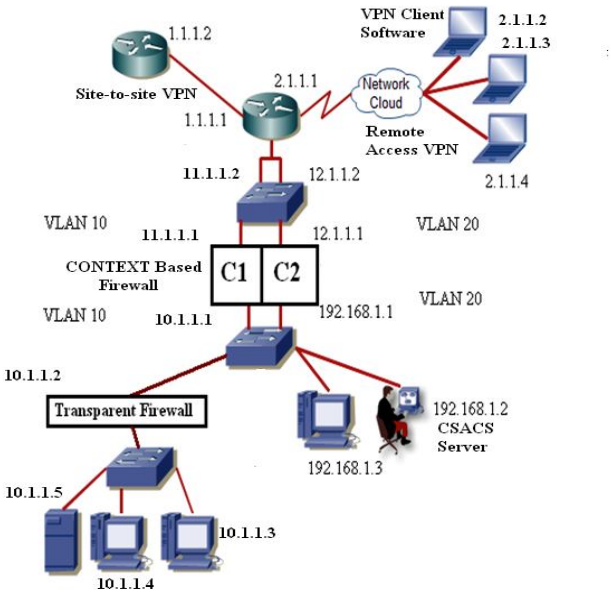


Fig. 10 Final Design Implemented

4. SOFTWARE ANALYSIS

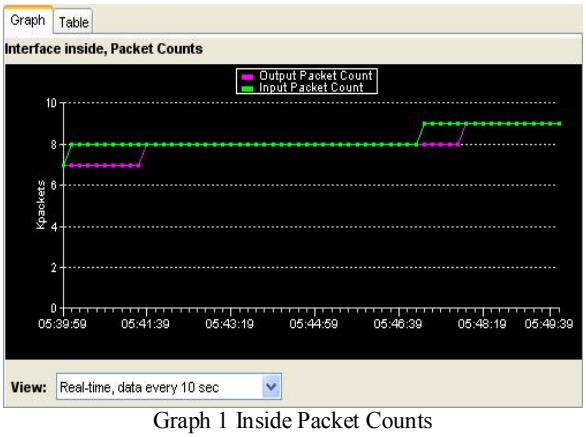
We have used ASDM, running on the context-based firewall, to evaluate the ICMP traffic flow from the inside users 10.1.1.3 and 10.1.1.4 of network 10.0.0.0 to the site-to-site VPN router. ASDM is a java applet used to configure and monitor the software on firewall. ASDM is loaded from the firewall and then used to configure, monitor and manage the device. Almost all CLI (Command Line Interface) commands are fully supported by ASDM, with only a few exceptions. Those commands are shown in ASDM GUI (Graphic Unit Interface) when they are added by CLI (Command Line Interface).

The Interface Graphs in ASDM are used to view interface statistics in graph or table form. If an interface is shared among contexts, the firewall shows only statistics for the current context [7].

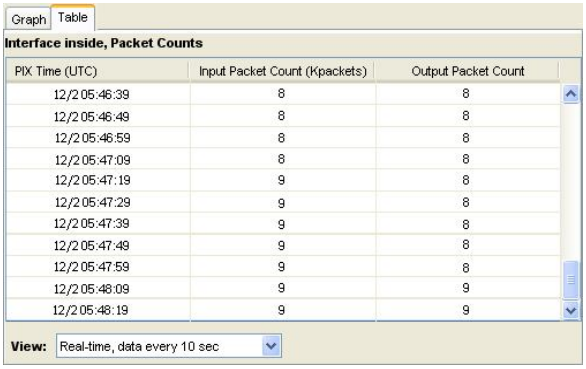
We can have up to four types of statistics to show in one graph window but we can open multiple graph windows at the same time. We have analyzed graphs at the inside interface and outside interface. Some of the available graphs are:

- Inside Packet Counts
- Inside Packet Rate
- Outside Packet Count
- Outside Packet Rate

Inside Packet Counts: It shows the number of packets input and output on the inside interface.



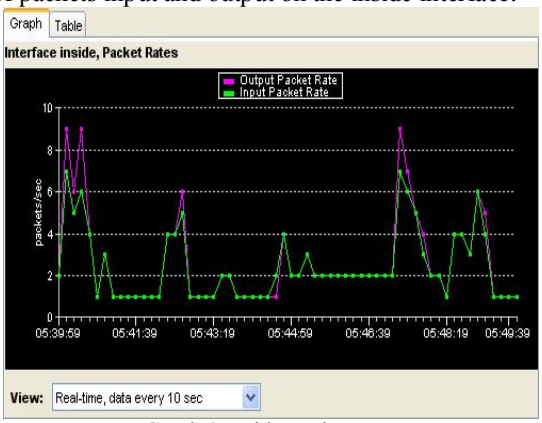
Graph 1 Inside Packet Counts



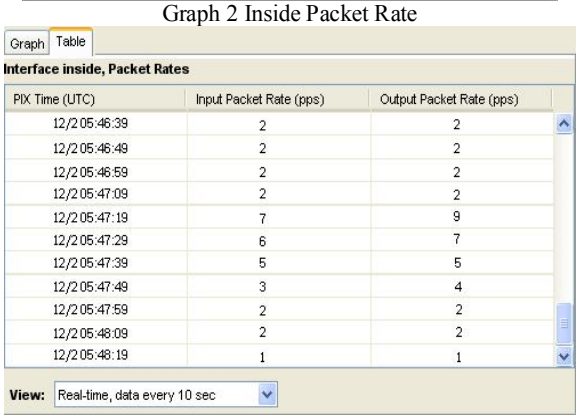
PIX Time (UTC)	Input Packet Count (Kpackets)	Output Packet Count
12/2 05:46:39	8	8
12/2 05:46:49	8	8
12/2 05:46:59	8	8
12/2 05:47:09	8	8
12/2 05:47:19	9	8
12/2 05:47:29	9	8
12/2 05:47:39	9	8
12/2 05:47:49	9	8
12/2 05:47:59	9	8
12/2 05:48:09	9	9
12/2 05:48:19	9	9

Table 1 Inside Packet Counts

Inside Packet Rate: It shows the rate of packets input and output on the inside interface.



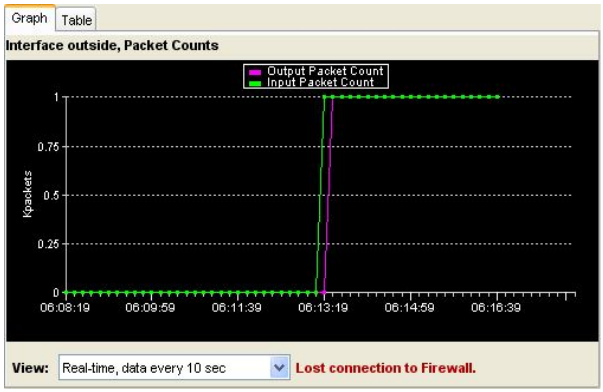
Graph 2 Inside Packet Rate



PIX Time (UTC)	Input Packet Rate (pps)	Output Packet Rate (pps)
12/2 05:46:39	2	2
12/2 05:46:49	2	2
12/2 05:46:59	2	2
12/2 05:47:09	2	2
12/2 05:47:19	7	9
12/2 05:47:29	6	7
12/2 05:47:39	5	5
12/2 05:47:49	3	4
12/2 05:47:59	2	2
12/2 05:48:09	2	2
12/2 05:48:19	1	1

Table 2 Inside Packet Rate

Outside Packet Counts: It shows the number of packets input and output on the outside interface.



Graph 3 Outside Packet Counts

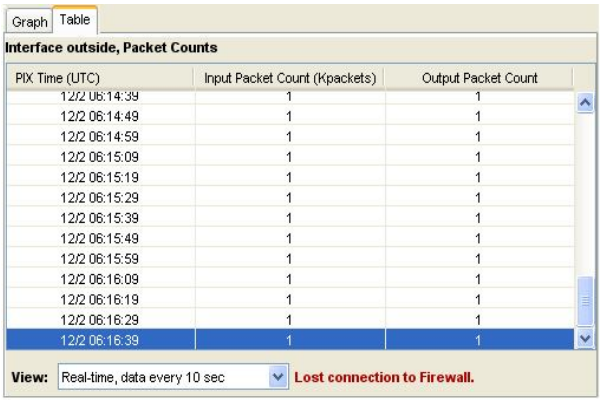
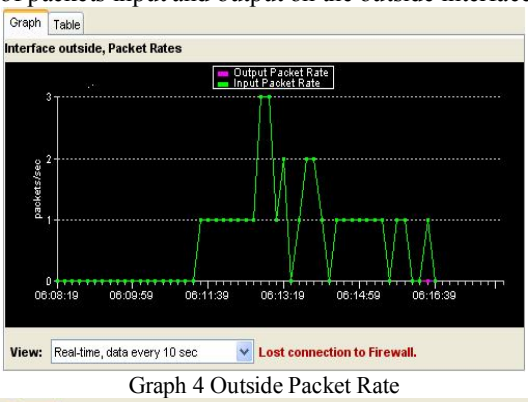


Table 3 Outside Packet Counts

Outside Packet Rate: It shows the rate of packets input and output on the outside interface.



Graph 4 Outside Packet Rate

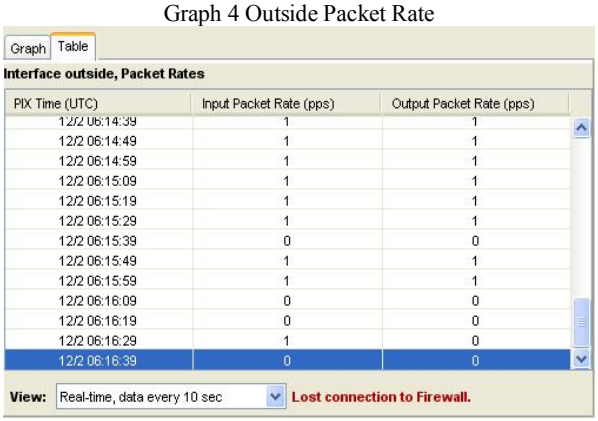


Table 4 Outside Packet Rate

5. CONCLUSION

Network Security has been a vital issue in this modern and ever developing network deployment around the globe. The increase in the users of IP based fast communication has made it essential to have reliable and fully secured data transfer between two points. As there is no physical boundary between networks so it is necessary to have much dynamic security arrangements to restrict unauthorized access to or from a specific network. The threat of misusing the internal access within that specific network is also there. We have designed such a sample network that could provide solution to these vulnerabilities of the network with the introduction of firewalls to restrict traffic flow "to or from" and within the network. At the end, to secure communication on shared public network, we use encryption and hashing techniques by forming logical tunnels known as VPNs. The work completed encompasses management of security in computer networks by combating network threats to provide secured data transmission on private and public networks.

REFERENCES

[1] Kenneth Ingham and Stephanie Forrest, 2002. A History and Survey of Network Firewalls, Technical Report, TRCS-2002-37, University New Mexico, 2002.

[2] David W. Chapman Jr., Andy Fox, 2001. Cisco Secure PIX Firewalls. Cisco Press, pp: 6-7.

[3] Christian Degu, 2003. CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide. Cisco Press, pp: 162-163.

[4] Ruixi Yuan, 2001. Virtual Private Networks: Technologies and Solutions. Addison Wesley Longman Publishing, pp: 113-121

[5] RFC854 Telnet Protocol Specification (http://tools.ietf.org/html/rfc854)

[6] RFC792 Internet Control Message Protocol (http://tools.ietf.org/html/rfc792)

[7] Cisco ASDM User Guide Manual, Cisco System Inc, Release 5.2

[8] Ray Blair, Arvind Durai, 2009. Cisco Secure Firewall Services Module (FWSM). Cisco Press, pp: 375-399.