IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 2, Issue 11, November 2014 ISSN 2321-5992

# VIRTUAL PRIVATE NETWORKS SERVER WITH FIREWALL TECHNIQUES AND ACCESS METHODS

**DR. P. RAJAMOHAN**

SENIOR LECTURER, SCHOOL OF INFORMATION TECHNOLOGY, SEGi UNIVERSITY, TAMAN SAINS SELANGOR, KOTA DAMANSARA, PJU 5, 47810 PJ, SELANGOR DARUL EHSAN, MALAYSIA.

## ABSTRACT

***A Virtual Private Network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A firewall is a piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy As viruses change after learning the language of a firewall, the firewall has to work even harder to keep up with these changes. With the same device we can connect to our Network via VPN and access our data from anywhere in the world. Keeping our data protected in a secure channel by using high encryption levels of protection. This paper presents the special issues of VPN technologies in communication especially firewall technologies and access methods supporting with VPNC standards and performance.***

**Keywords:-** VPN - Virtual Private Network, PPTP - Point-to-Point Tunneling Protocol, L2TP - Layer Two Tunneling Protocol , TCP - Transmission Control Protocol, NAS - Network Access Server, IP - Internet Protocols.

## 1. INTRODUCTION

Using VPNs, an organization can help secure private network traffic over an unsecured network, such as the Internet. VPN helps provide a secure mechanism for encrypting and encapsulating private network traffic and moving it through an intermediate network. Data is encrypted for confidentiality, and packets that might be intercepted on the shared or public network are indecipherable without the correct encryption keys. Data is also encapsulated, or wrapped, with an IP header containing routing information. VPNs help enable users working at home, on the road, or at a branch office to connect in a secure fashion to a remote corporate server using the Internet. From the users perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate network, the Internet, is irrelevant to the user because it appears as if the data is being sent over a dedicated private link[1].

## 2. TYPES OF VPN CONNECTION

### 2. 1 Remote access VPN

A remote access VPN connection is made by a remote access client. A remote access client is a single computer user who connects to a private network from a remote location. The VPN server provides access to the resources of the network to which the VPN server is connected. The packets sent across the VPN connection originate at the VPN client. The VPN client authenticates itself to the VPN server and, for mutual authentication, the VPN server authenticates itself to the VPN client[1].

### 2.2 Site-to-site VPN

A site-to-site VPN connection connects two portions of a private network or two private networks. For example, this allows an organization to have routed connections with separate offices, or with other organizations, over the Internet. A routed VPN connection across the Internet logically operates as a dedicated Wide Area Network (WAN) link. The VPN server provides a routed connection to the network to which the VPN server is attached. On a site-to-site VPN connection, the packets sent from either router across the VPN connection typically do not originate at the routers. The calling router (the VPN client) authenticates itself to the answering router (the VPN server), and, for mutual authentication, the answering router authenticates itself to the calling router[1].

### 2.3 Internet-based VPN Connections

Using an Internet-based VPN connection, an organization can avoid long-distance charges while taking advantage of the global availability of the Internet[2].

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 2, Issue 11, November 2014 ISSN 2321-5992

**2.3.1 Remote Access VPN Connections over the Internet**

A remote access VPN connection over the Internet enables a remote access client to initiate a dial-up connection to a local ISP instead of connecting to a corporate or outsourced network access server (NAS). By using the established physical connection to the local ISP, the remote access client initiates a VPN connection across the Internet to the organization's VPN server. When the VPN connection is created, the remote access client can access the resources of the private intranet. The following figure shows remote access over the Internet[2].

**2.3.2 VPN Connecting a Remote Client to a Private Intranet**

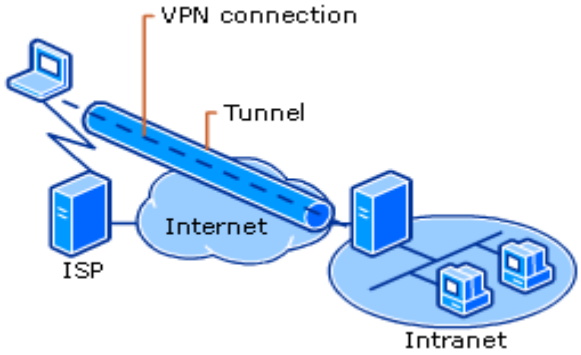


**Figure 1:** VPN Connecting a Remote Client to a Private Intranet

**2.3.3 Site-to-Site VPN Connections Over the Internet**

When networks are connected over the Internet, as shown in the following figure, a router forwards packets to another router across a VPN connection. To the routers, the VPN connection operates as a data-link layer link.[2]

**2.3.4 VPN Connecting Two Remote Sites Across the Internet**

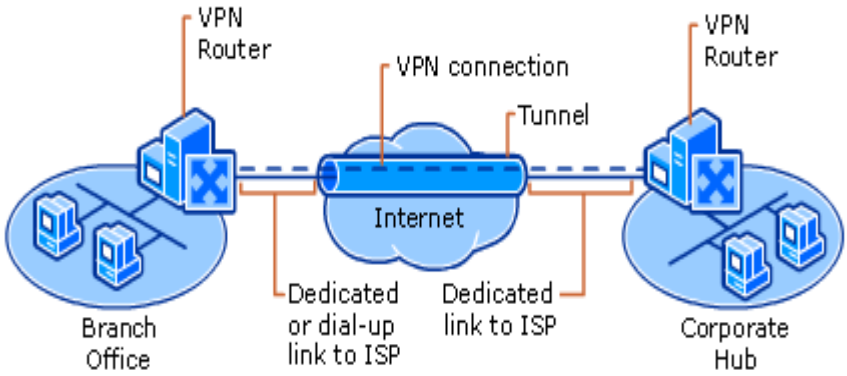


**Figure 2:** VPN Connecting Two Remote Sites Across the Internet

**2.4 Intranet-based VPN Connections**

The intranet-based VPN connection takes advantage of IP connectivity in an organization's Local Area Network (LAN).

**2.4.1 Remote Access VPN Connections over an Intranet**

In some organization intranets, the data of a department, such as human resources, is so sensitive that the network segment of the department is physically disconnected from the rest of the intranet. While this protects the data of the human resources department, it creates information accessibility problems for authorized users not physically connected to the separate network segment. VPN connections help provide the required security to enable the network segment of the human resources department to be physically connected to the intranet. In this configuration, a VPN server can be used to separate the network segments. The VPN server does not provide a direct routed connection between the corporate intranet and the separate network segment. Users on the corporate intranet with appropriate permissions can establish a remote access VPN connection with the VPN server and gain access to the protected resources. Additionally, all communication across the VPN connection is encrypted for data confidentiality. For those users who are not authorized to establish a VPN connection, the separate network segment is hidden from view. The following figure shows remote access over an intranet.[1][2]

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 2, Issue 11, November 2014 ISSN 2321-5992

**2.4.2 VPN Connection Allowing Remote Access to a Secured Network over an Intranet**

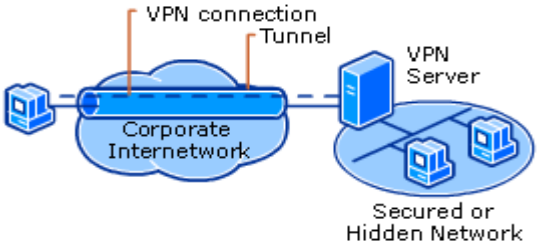


**Figure 3:** VPN Connection Allowing Remote Access to a Secured Network over an Intranet

**2.4.3 Site-to-Site VPN Connections over an Intranet**

Two networks can be connected over an intranet using a site-to-site VPN connection. This type of VPN connection might be necessary, for example, for two departments in separate locations, whose data is highly sensitive, to communicate with each other. For instance, the finance department might need to communicate with the human resources department to exchange payroll information. The finance department and the human resources department are connected to the common intranet with computers that can act as VPN clients or VPN servers. When the VPN connection is established, users on computers on either network can exchange sensitive data across the corporate intranet. The following figure shows two networks connected over an intranet.[1][2]

**2.4.4 VPN Connecting Two Networks over an Intranet**

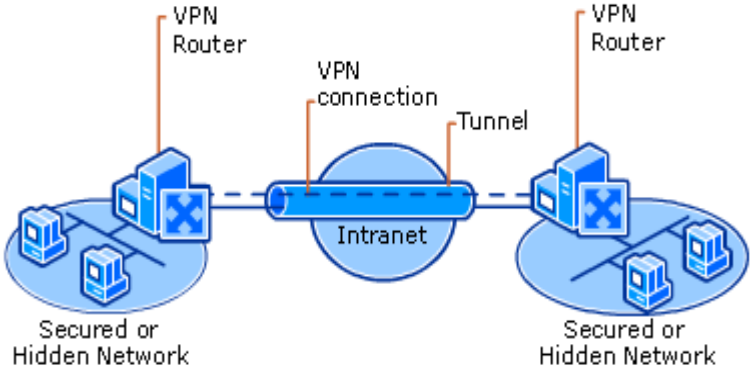


**Figure 4:** VPN Connecting Two Networks over an Intranet

## 3. VPN FIREWALL ARCHITECTURE TECHNIQUES

### 3.1 VPN and Firewalls

A firewall uses packet filtering to allow or disallow the flow of specific types of network traffic. IP packet filtering provides a way for administrators to define precisely what IP traffic is allowed to cross the firewall. IP packet filtering is important when private intranets are connected to public networks, such as the Internet. There are two approaches to using a firewall with a VPN server:[3][4]

- A firewall is between the VPN server and the Internet. In this configuration, the VPN server is behind the firewall.
- The VPN server is connected to the Internet and the firewall is between the VPN server and the intranet. In this configuration, the VPN server is in front of the firewall.

### 3.2 Firewall-Based VPNs

With firewall-based VPNs, it is considered a safe presumption that a firewall will be used and placed at the network perimeter, as illustrated in Figure 5:.

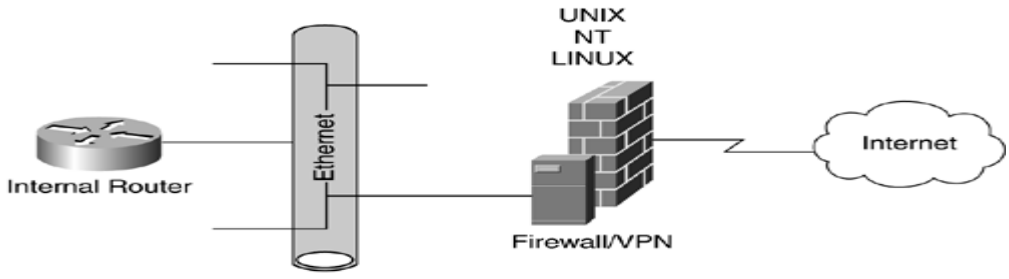


**Figure 5:.** Firewall-Based VPN

This presumption leads to a natural extension that this device also can support the VPN connections, providing a central point of management of both the firewall and network access security policies. A drawback to this combined

firewall/VPN-access method is performance. On a single "box," a busy Internet circuit with multiple VPNs could overload the system.

**3.3 Black-Box-Based VPNs**

In the black-box scenario, a vendor offers just that, a black box; a device loaded with encryption software to create a VPN tunnel. Black-box VPN vendors should be supporting all three tunneling protocols - PPTP, L2TP, and IPSec. Specific vendors need to be thoroughly researched, however, because they don't all provide the same level of tunneling protocol support. The black-box VPN sits behind or with the firewall, as illustrated in Figure 6:[5].

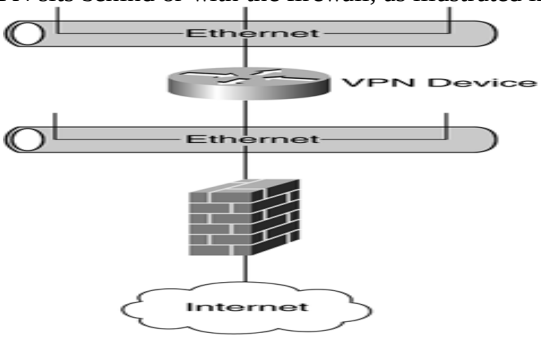


**Figure 6:.** Black-Box-Based VPN

The firewall provides security to the organization, not the data, whereas the VPN device provides security to the data, but not the organization. If the firewall is in front of the VPN device, a rule-based policy on that firewall will need to be implemented.

**3.4 VPN Server Behind a Firewall**

In the configuration shown in the following figure 7, the firewall is connected to the Internet and the VPN server is another intranet resource connected to the perimeter network, also known as a screened subnet or demilitarized zone (DMZ). The perimeter network is an IP network segment that typically contains resources available to Internet users such as Web servers and FTP servers. The VPN server has an interface on the perimeter network and an interface on the intranet. In this approach, the firewall must be configured with input and output filters on its Internet and perimeter network interfaces to allow the passing of tunnel maintenance traffic and tunneled data to the VPN server. Additional filters can allow the passing of traffic to Web servers, FTP servers, and other types of servers on the perimeter network. As an added layer of security, the VPN server should also be configured with PPTP or L2TP/IPSec packet filters on its perimeter network interface as described in “VPN Server in Front of a Firewall” in this section. Because the firewall does not have the encryption keys for each VPN connection, it can only filter on the plaintext headers of the tunneled data, meaning that all tunneled data passes through the firewall.[3]-[5][8]

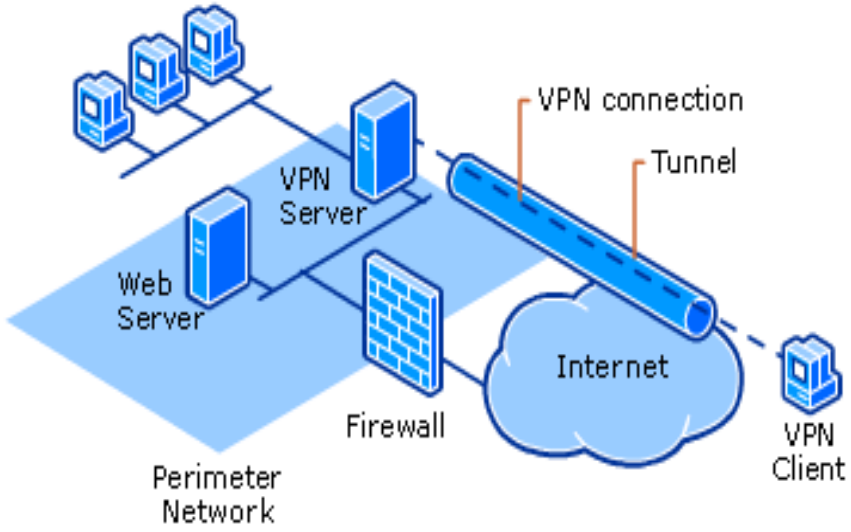


**Figure 7:** VPN Server Behind the Firewall

**3.4.1 Packet Filters for a VPN Server Behind a Firewall**

If the VPN server is behind a firewall, packet filters must be configured for both an Internet interface and a perimeter network interface. In this scenario, the firewall is connected to the Internet, and the VPN server is an intranet resource

that is connected to the perimeter network. The VPN server has an interface on both the perimeter network and the Internet.

**3.4.2 VPN Server Behind a Firewall: PPTP Filters on the Firewall's Internet Interface**

PPTP connections for the Internet interface of the firewall.

The following Table 1: Shows the inbound and outbound PPTP filters on the firewall's Internet interface.[5][8]

**Table 1:**

| Filter Type | Filter | Action |
|---|---|---|
| Inbound | **Destination IP address** = Perimeter network interface of VPN server<br>**TCP destination port**= 1723 (0x6BB) | Allows PPTP tunnel maintenance traffic from the PPTP client to the PPTP server. |
| Inbound | **Destination IP address** = Perimeter network interface of VPN server<br>**IP Protocol ID** = 47 (0x2F) | Allows tunneled PPTP data from the PPTP client to the PPTP server. |
| Inbound | **Destination IP address** = Perimeter network interface of VPN server<br>**TCP source port** = 1723 (0x6BB) | Required only when the VPN server is acting as a VPN client (a calling router) in a site-to-site VPN connection. If all traffic from TCP port 1723 is allowed to reach the VPN server, network attacks can emanate from sources on the Internet that use this port. Administrators should only use this filter in conjunction with the PPTP filters that are also configured on the VPN server. |
| Outbound | **Source IP address** = Perimeter network interface of VPN server<br>**TCP source port** = 1723 (0x6BB) | Allows PPTP tunnel maintenance traffic from the PPTP server to the PPTP client. |
| Outbound | **Source IP address** = Perimeter network interface of VPN server<br>**IP Protocol ID** = 47 (0x2F) | Allows tunneled PPTP data from the PPTP server to the PPTP client. |
| Outbound | **Source IP address** = Perimeter network interface of VPN server<br>**TCP destination port**= 1723 (0x6BB) | Required only when the VPN server is acting as a VPN client (a calling router) in a site-to-site VPN connection. If all traffic from the VPN server is allowed to reach TCP port 1723, network attacks can emanate from sources on the Internet using this port. Administrators should only use this filter in conjunction with the PPTP filters that are also configured on the VPN server. |

**3.4.3 VPN Server Behind a Firewall: PPTP Filters on the Perimeter Network Interface**

PPTP connections for the perimeter network interface of the firewall. The following Table 2: Shows the inbound and outbound PPTP filters on the firewall's perimeter network interface.[5][8]

**Table 2:**

| Filter Type | Filter | Action |
|---|---|---|
| Inbound | **Source IP address** = Perimeter network interface of VPN server **TCP source port** = 1723 (0x6BB) | Allows PPTP tunnel maintenance traffic from the VPN server to the VPN client. |
| Inbound | **Source IP address** = Perimeter network interface of VPN server **IP Protocol ID** = 47 (0x2F) | Allows tunneled PPTP data from the VPN server to the VPN client. |
| Inbound | **Source IP address** = Perimeter network interface of VPN server **TCP destination port** = 1723 (0x6BB) | Required only when the VPN server is acting as a VPN client (a calling router) in a site-to-site VPN connection. If all traffic from TCP port 1723 is allowed to reach the VPN server, network attacks can emanate from sources on the Internet using this port. |
| Outbound | **Destination IP address** = Perimeter network interface of VPN server **TCP source port** = 1723 (0x6BB) | Allows PPTP tunnel maintenance traffic from the PPTP client to the PPTP server. |
| Outbound | **Destination IP address** = Perimeter network interface of VPN server **IP Protocol ID** = 47 (0x2F) | Allows tunneled PPTP data from the PPTP client to the PPTP server. |
| Outbound | **Destination IP address** = Perimeter network interface of VPN server **TCP source port** = 1723 (0x6BB) | Required only when the VPN server is acting as a VPN client (a calling router) in a site-to-site VPN connection. If all traffic from the VPN server is allowed to reach TCP port 1723, network attacks can emanate from sources on the Internet using this port. |

**3.4.4 VPN Server Behind a Firewall: L2TP/IPSec Filters on the Firewall's Internet Interface**

L2TP/IPSec connections for the Internet interface of the firewall. The following Table 3: Shows the inbound and outbound L2TP/IPSec filters on the firewall's Internet interface.[5][8]

**Table 3:**

| Filter Type | Filter | Action |
|---|---|---|
| Inbound | **Destination IP address** = Perimeter network interface of VPN server **UDP destination port** = 500 (0x1F4) | Allows IKE traffic to the VPN server. |
| Inbound | **Destination IP address** = Perimeter network interface of VPN server **UDP destination port** = 4500 (0x1194) | Allows IPSec NAT-T traffic to the VPN server. |
| Inbound | **Destination IP address** = Perimeter network interface of | Allows IPSec ESP traffic to the VPN |

| | | |
|---|---|---|
| | VPN server **IP Protocol ID** = 50 (0x32) | server. |
| Outbound | **Source IP address** = Perimeter network interface of VPN server **UDP source port** = 500 (0x1F4) | Allows IKE traffic from the VPN server. |
| Outbound | **Source IP address** = Perimeter network interface of VPN server **UDP source port** = 4500 (0x1194) | Allows IPSec NAT-T traffic from the VPN server. |
| Outbound | **Source IP address** = Perimeter network interface of VPN server **IP Protocol ID** = 50 (0x32) | Allows IPSec ESP traffic from the VPN server. |

No filters are required for L2TP traffic at UDP port 1701. All L2TP traffic at the firewall, including tunnel maintenance and tunneled data, is encrypted with IPSec ESP.

**3.4.5 VPN Server Behind a Firewall: L2TP/IPSec Filters on the Firewall's Perimeter Network Interface**

L2TP/IPSec connections for the perimeter network interface of the firewall.

The following Table 4: Shows the inbound and outbound L2TP/IPSec filters on the firewall's perimeter network interface.[5][8]

**Table 4:**

| Filter Type | Filter | Action |
|---|---|---|
| Inbound | **Source IP address** = Perimeter network interface of VPN server **UDP source port** = 500 (0x1F4) | Allows IKE traffic from the VPN server. |
| Inbound | **Source IP address** = Perimeter network interface of VPN server **UDP source port** = 4500 (0x1194) | Allows IPSec NAT-T traffic from the VPN server. |
| Inbound | **Source IP address** = Perimeter network interface of VPN server **IP Protocol ID** = 50 (0x32) | Allows IPSec ESP traffic from the VPN server. |
| Outbound | **Destination IP address** = Perimeter network interface of VPN server **UDP destination port** = 500 (0x1F4) | Allows IKE traffic to the VPN server. |
| Outbound | **Destination IP address** = Perimeter network interface of VPN server **UDP destination port** = 4500 (0x1194) | Allows IPSec NAT-T traffic to the VPN server. |
| Outbound | **Destination IP address** = Perimeter network interface of VPN server **IP Protocol ID** = 50 (0x32) | Allows IPSec ESP traffic to the VPN server. |

**3.5 VPN Server in Front of a Firewall**

With the VPN server in front of the firewall and connected to the Internet, as shown in the following figure, administrators need to add packet filters to the Internet interface that allow only VPN traffic to and from the IP address of the VPN server's interface on the Internet. For inbound traffic, when the tunneled data is decrypted by the VPN server it is forwarded to the firewall, which employs its filters to allow the traffic to be forwarded to intranet resources. Because the only traffic that is crossing the VPN server is traffic generated by authenticated VPN clients, firewall filtering in this scenario can be used to prevent VPN users from accessing specific intranet resources. Because the only Internet traffic allowed on the intranet must go through the VPN server, this approach also prevents the sharing of intranet resources with non-VPN Internet users.[5]-[8]

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation .....
Email: editoriijcs@ipasj.org
Volume 2, Issue 11, November 2014
ISSN 2321-5992

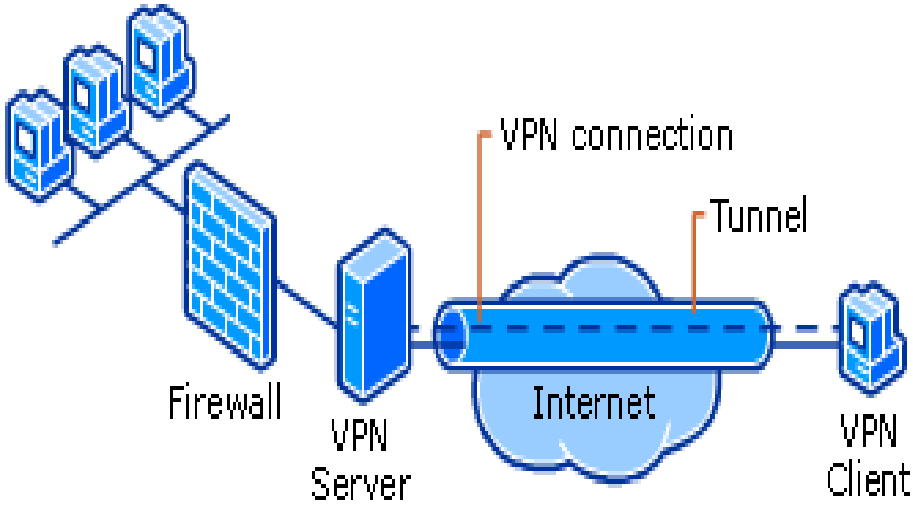


**Figure 8:** VPN Server in Front of the Firewall

**3.5.1 Packet Filters for a VPN Server in Front of a Firewall**

When a VPN server is in front of a firewall and connected to the Internet, inbound and outbound packet filters on the VPN server need to be configured to allow only VPN traffic to and from the IP address of the VPN server's Internet interface. Use this configuration if the VPN server is in a perimeter network, with one firewall positioned between the VPN server and the intranet and another between the VPN server and the Internet. All of the following packet filters are configured, using the Routing and Remote Access snap-in, as IP packet filters on the Internet interface. Depending on the configuration decisions made when running the Routing and Remote Access Server Setup Wizard, these packet filters might already be configured. [3][5]-[8]

**3.5.2 VPN Server in Front of a Firewall: PPTP Packet Filters on the Internet Interface**

PPTP connections for the inbound and outbound filters. The following Table 5: Shows the VPN server's inbound and outbound filters for PPTP.[5]-[8]

**Table 5:**

| Filter Type | Filter | Action |
|---|---|---|
| Inbound | **Destination IP address** = Internet interface of VPN server<br>**Subnet mask** = 255.255.255.255<br>**TCP destination port** = 1723 | Allows PPTP tunnel maintenance to the VPN server. |
| Inbound | **Destination IP address** = Internet interface of VPN server<br>**Subnet mask** = 255.255.255.255<br>**IP Protocol ID** = 47 | Allows tunneled PPTP data to the VPN server. |
| Inbound | **Destination IP address** = Internet interface of VPN server<br>**Subnet mask** = 255.255.255.255<br>**TCP (established) source port** = 1723 | Required only when the VPN server is acting as a VPN client (a calling router) in a site-to-site VPN connection. Accepts TCP traffic only when a VPN server initiates the TCP connection. |
| Outbound | **Source IP address** = Internet interface of VPN server<br>**Subnet mask** = 255.255.255.255<br>**TCP source port** = 1723 | Allows PPTP tunnel maintenance traffic from the VPN server. |
| Outbound | **Source IP address** = Internet interface of VPN | Allows tunneled PPTP data from the VPN server. |

| | | |
|---|---|---|
| | server<br>**Subnet mask** = 255.255.255.255<br>**IP Protocol ID** = 47 | |
| Outbound | **Source IP address** = Internet interface of VPN server<br>**Subnet mask** = 255.255.255.255<br>**TCP (established) destination port**= 1723 | Required only when the VPN server is acting as a VPN client (a calling router) in a site-to-site VPN connection. Sends TCP traffic only when a VPN server initiates the TCP connection. |

**3.5.3 VPN Server in Front of a Firewall: L2TP/IPSec Packet Filters on the Internet Interface**
L2TP/IPSec connections . The following Table 6:shows the VPN server's inbound and outbound filters for L2TP/IPSec [5]-[8].

**Table 6:**

| Filter Type | Filter | Action |
|---|---|---|
| Inbound | **Destination IP address** = Internet interface of VPN server<br>**Subnet mask** = 255.255.255.255<br>**UDP destination port** = 500 | Allows IKE traffic to the VPN server. |
| Inbound | **Destination IP address** = Internet interface of VPN server<br>**Subnet mask** = 255.255.255.255<br>**UDP destination port** = 1701 | Allows L2TP traffic from the VPN client to the VPN server. |
| Inbound | **Destination IP address** = Internet interface of VPN server<br>**Subnet mask** = 255.255.255.255<br>**UDP destination port** = 4500 | Allows IPSec NAT-T traffic from the VPN client to the VPN server. |
| Outbound | **Source IP address** = Internet interface of VPN server<br>**Subnet mask** = 255.255.255.255<br>**UDP source port** = 500 | Allows IKE traffic from the VPN server. |
| Outbound | **Source IP address** = Internet interface of VPN server<br>**Subnet mask** = 255.255.255.255<br>**UDP source port** = 1701 | Allows L2TP traffic from the VPN server to the VPN client. |
| Outbound | **Source IP address** = Internet interface of VPN server<br>**Subnet mask** = 255.255.255.255<br>**UDP source port** = 4500 | Allows IPSec NAT-T traffic from the VPN server to the VPN client |

## 4. CONCLUSION

VPN can be a solution to reduce the network complexity, reduce the networks operational cost and access the remote network via global Internet or Intranet with support of VPN Technologies. IPsec is the most dominant protocol for secure VPNs. SSL gateways for remote-access users are also popular for secure VPNs. L2TP running under IPsec has a

much smaller but significant deployment. Encryption and authentication protocols keep corporate information private on public networks. A firewall is a piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy As viruses change after learning the language of a firewall, the firewall has to work even harder to keep up with these changes. With the same device we can connect to our Network via VPN and access our data from anywhere in the world. Keeping our data protected in a secure channel by using high encryption levels of protection with VPN technologies, new users can be easily added to the network. Corporate network availability can be scaled quickly with minimal cost.

## REFERENCES

[1] Dave Kosiur, Wiley & Sons, "Building and Managing Virtual Private Networks"; ISBN: 0471295264, pp. 35-110.
[2] Dr.S.S.Riaz Ahamed & P.Rajamohan, "Comprehensive performance Analysis and special issues of Virtual Private Network Strategies in the computer Communication: a Novel Study", International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462 Vol. 3 No. 7 July 2011, pp. 640-648.
[3] Wei Luo, Carlos Pignataro, Dmitry Bokotey, Anthony Chan (Cisco Press 2005), "Layer 2 VPN Architectures", pp.73-122.
[4] Chris Metz., "The Latest in Virtual Private Networks: Part II. IEEE Internet Computing", pp. 60–65, 2004.
[5] Cisco Press, Network Sales and Services Handbook (Cisco Press Networking Technology) - Chapter - Firewall.
[6] Ronald, F.J. (Ed 2003). "CCSP Cisco Secure VPN. VPN Over IPSec.", pp. 36-39.
[7] Ronald, F.J. (Ed 2003). "CCSP Cisco Secure VPN. Explanation of the IPSec protocols", pp. 39-45..
[8] Sources : Microsoft tech net from Website- Article : VPN firewalls Approach.

**AUTHOR**

**DR. P. RAJAMOHAN** received his Bachelor of Science Degree in Physics later he obtained his Post Graduate Diploma in Computer Applications (PGDCA), Master Degree in Computer Applications (MCA) and PhD in Computer Science. His primary research interest in Virtual Private Network Implementation for Efficient Data Communication and wireless Networks Communications. He is the member of the Institution of Engineers (India), member of Associate in Cisco Certified Networks and member of the International Association of Engineers (IAENG). Dr. P. Rajamohan, over all his 20 years experiences in both academic and IT industry. He is currently working as a Senior Lecturer in School of Information Technology, SEGi University, Malaysia.