Proper Virtual Private Network (VPN) Solution

Conference Paper · October 2008

DOI: 10.1109/NGMAST.2008.18 · Source: IEEE Xplore

3 authors, including:

Ahmed A. Jaha
College of Industrial Technology, Mişrātah, Libya
9 PUBLICATIONS **39** CITATIONS
SEE PROFILE

Majdi Ashibani
Libyan ICT Academy
23 PUBLICATIONS **72** CITATIONS
SEE PROFILE

Proper Virtual Private Network (VPN) Solution

Ahmed A. Jaha, Fathi Ben Shatwan, and Majdi Ashibani
The Higher Institute of Industry, Misurata, Libya
goha_99@yahoo.com

Abstract

A Virtual Private Network (VPN) can be defined as a way to provide secure communication between members of a group through use of public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. There are many different VPN solutions out there, and just deciding which one to choose can be difficult since they all have advantages and disadvantages. VPNs can be categorized as Secure or Trusted VPNs, Client-based or Web-based VPNs, Customer Edge-based or Provider Edge-based VPNs, or Outsourced or In-house VPNs. These categories often overlap each other. In order to decide what VPN solutions to choose for different parts of the enterprise infrastructure, the chosen solution should be the one that best meets the requirements of the enterprise. The purpose of this paper is to serve as a basis when creating an enterprise WAN which connects sites and users together using VPN technology. The purpose of creating such a WAN is to allow the resources of a company to be remotely accessed.

1. Introduction

In the past, organizations or enterprises would physically install lines over large distances to ensure secure data transfer. However, this system is impractical for every enterprise and everyday users due to the cost, space, and time required for such installations. In recent years, with the exponential growth of the Internet, the landscape of telecommunications has changed radically and the Internet has become part of almost every aspect of the developed world including education, banking, business, and politics. Over the past two decades the public Internet has been found to be vulnerable to attackers seeking sensitive information. The most recent solution to this problem has been IP-based Virtual Private Network (IPVPN). A Virtual Private Network (VPN) can be defined as a way to provide secure communication between members of a group through use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. VPN systems provide users with the illusion of a completely private network. An IP Virtual Private Network (IPVPN) can be defined as a VPN implementation that uses public or shared IP network resources to emulate the characteristics of an IP-based private network.

The main purpose of a VPN is to give enterprises the same capabilities, or even better, as in private networks, but at a much lower cost. Enterprises benefit from VPN in reducing the cost, increasing the scalability, and increasing the productivity, with out impairing the security [1].

VPN should provide authentication, access control, confidentiality, and data integrity to ensure security of the data.

A VPN should typically support the architecture that is consists from main LAN at the headquarters of an enterprise, other LANs at remote offices, partner or customer company LANs, and individual users connecting from out in the field. There are basically two types of VPNs, remote access VPN and site-to-site VPN. Site to site VPN can be further divided into intranet VPN and extranet VPN.

2. Remote Access VPN Protocols

To establish a connection, both the client and the server must be using the same VPN protocol [2].

2.1. Point to Point Tunneling Protocol (PPTP)

PPTP is a standard tunneling protocol developed by PPTP Forum which consists of Microsoft and some other remote access vendors [3].

2.2. Layer Two Tunneling Protocol (L2TP)

L2TP is a combination of PPTP and Layer Two Forwarding (L2F) developed by IETF [4].

2.3. Internet Protocol Security (IPSec)

IPSec is a framework of IETF open standards aim at securing traffic on the network layer [5].

2.4. Secure Socket Layer (SSL)

SSL is a higher-layer security protocol developed by Netscape. SSL is commonly used with HTTP to enable secure Web browsing, called HTTPS [6].

2.5. Multi Protocol Label Switching (MPLS)

MPLS is a label-based packet switching technique that has evolved from numerous prior technologies such as Cisco's "Tag Switching" and IBM's "ARIS". The idea is that a small label, or stack of labels, is inserted between the data link and network layer headers to make efficient routing decisions [7].

3. Vpn Classification

There are wide variety types of possible VPNs. In this section, we give a brief description for some of the VPNs appeared in the literature. Please note that it is difficult to precisely divide them into different categories. There are potential overlaps between some of the VPNs. The technologies can be classified in several ways. Some of these ways are described in this paper as shown in table (1)

Table(1) Classification of VPN technologies

<table>
<tr><td colspan="8">VPN solutions</td></tr>
<tr><td colspan="5">In-house</td><td colspan="3">Out-source</td></tr>
<tr><td colspan="6">CE-based</td><td colspan="2">PE-based</td></tr>
<tr><td colspan="7">Secure</td><td>Trusted</td></tr>
<tr><td colspan="4">Client-based</td><td colspan="3">Web-based</td><td rowspan="2">MPLS</td></tr>
<tr><td>PPTP</td><td>L2TP</td><td>IPSec</td><td colspan="4">SSL</td></tr>
</table>

3.1. Trusted and Secure VPNs

According to this categorization, which is supported by the VPN Consortium (VPNC) [8], VPN solutions can be divided into secure, trusted and hybrid VPNs.

Trusted VPNs consist of one or more paths leased from a service provider. These VPNs usually originate and terminate in the provider's network. The privacy and integrity afforded by trusted VPNs is only that the service provider assures the customer that no one else is using the same path. MPLS is an example of technologies used in trusted VPNs.

Secure VPNs are constructed using encryption and other security mechanisms (e.g. authentication, integrity checking). The traffic is encrypted at the network edge or sending computer, before moving over the Internet, and then decrypted when it reaches the enterprise network or a receiving computer. Creating a secure VPN often includes purchasing, configuring and maintaining hardware and software. Examples of secure VPN technologies are PPTP, L2TP, IPSec and SSL.

It should be stated that trusted VPNs do not prohibit security. If confidentiality is an issue, traffic can be encrypted before it is sent through the trusted VPN, thus creating a hybrid solution between trusted and secure VPNs. Secure VPNs provide security but no assurance of paths. Trusted VPNs provide assurance of properties of paths such as QoS, but no security from snooping or alteration. Because of these strengths and weaknesses, hybrid VPNs have started to appear.

3.2. Web-based and Client-based VPNs

They are often used to support remote access users. This does not necessarily mean that the two solutions compete with each other. Rather, they complement each other.

Web-based VPNs are based on SSL, which is considered to be the standard web-based VPNs technology today. Any computer with a web browser installed on it can, thereby, be used to connect to the enterprise network after the user has been authenticated. Web-based VPN solution reduces any cost associated with purchasing, installing, and maintaining the client software. Web-based VPNs typically support a limited set of Web applications.

Client-based VPNs are based on PPTP, L2TP, IPSec and SSL. Client-based VPNs require a client software to be installed on each host that is remotely connecting to the enterprise network. Client based VPNs allow remote access users to get the seamless access to the enterprise network from their PCs. Client-based VPN solution requires purchasing, installing, and maintaining the client software.

3.3. PE-based and CE-based VPNs

In CE-based VPNs, all the VPN processing takes place in the CE devices. A tunnel is simply created between the CE devices, and the PE devices can be standard routers and switches. With CE-based VPNs, CE devices require a high amount of management and configuration. Usually, the equipments on the customer premises need to be upgraded or purchased.

In PE-based VPNs, all the VPN processing takes place in the PE devices. When employing this solution, the CE devices can be standard routers and switches. The VPN management and configuration takes place in the PE devices. So, there is usually no need to upgrade the equipments on the customer premises.

3.4. Outsourced and In-house VPNs

Although many enterprises build their own VPNs, many others outsource their VPNs to managed VPN providers. These providers, most of which are ISPs, install all necessary hardware, do configuration, and manage the customer's VPNs on an ongoing basis. Outsourcing reduces the skills an enterprise's security staff must have and reduces internal security labor costs. It also gives predicable costs. However, enterprises that outsource their VPNs lose control over their VPN security. In addition, outsourced VPNs can cost more than internally built and managed VPNs. Especially if the number of remote users and branch offices are increasing (since these solutions often charge per user).

4. Choosing Proper Vpn Solution

In order to decide what VPN solutions to choose for different parts of the enterprise infrastructure, the chosen solution should be the one that best meets the requirements of the enterprise. We will start by ruling out those that are not suitable.

4.1 Choosing Proper Remote Access VPN Solution

When providing remote access VPN solution, all other alternatives than web-base VPN solution which is based on SSL VPN and client-based VPN solution which is based on PPTP, L2TP, IPSec, or SSL VPNs can be ruled out. Obviously trusted VPN solution which is based on MPLS VPN is ruled out because it would be impossible to extend

MPLS network to each remote access user. Even if cost would not be an issue, remote access with trusted VPN solution which is based on MPLS VPN could only be supported to fixed locations and mobility would thus not be supported at all.

4.1.1 Access requirements

Web-based VPN solution which is based on SSL VPN is well suited for remote access connections with low access requirements in which remote access users need access to the Web-based applications such as online catalogues, price lists, order entry, customer contact reporting, or similar applications.

Client-based VPN solution which is based on PPTP, L2TP, IPSec, or SSL VPNs is a good choice for remote access connections with high access requirements in which remote access users need access to the entire or large portions of the enterprise network. In this situation the remote access users can get the seamless access to the enterprise network from their PCs. This means that network drives can be mapped directly into the computer, providing access to network-based files from any application.

4.1.2 Security requirements

Client-based VPN solution which is based on PPTP or L2TP VPNs is a good choice for remote access connections with low security requirements, since the used authentication and encryption algorithms are weak [2] [9].

Client-based VPN solution which is based on IPSec or SSL VPNs or Web-based VPN solution which is based on SSL VPN is a good choice for remote access connections with high security requirements, since both of them are using strong authentication and encryption algorithms [2] [10].

4.1.3 Protocols support requirements

Client-based VPN solution which is based on IPSec or SSL VPNs or Web-based VPN solution which is based on SSL VPN is a good choice for remote access connections with low protocols support requirements, where the only packets of TCP/IP network protocol are forwarded through the WAN.

Client-based VPN solution which is based on PPTP or L2TP VPNs is a good choice for remote access connections with high protocols support requirements, where the packets of multiple network protocols such as TCP/IP, IPX/SPX, or NetBEUI are forwarded through the WAN.

4.1.4 Cost requirements

Web-based VPN solution which is based on SSL VPN is well suited for remote access connections with low cost requirements, since there is only need to web browser in order to establish connection to the enterprise network.

Client-based VPN solution which is based on PPTP, L2TP, IPSec, or SSL VPNs is well suited for remote access connections with high cost requirements, since there is a need to install or configure a client in order to establish connection to the enterprise network.

4.1.5 Remote Access VPN Matrix

Table (2) shows the remote access VPN Matrix That is used to help enterprises for selecting the proper remote access VPN solution.

Table (2) Remote Access VPN Matrix

Requirements	Value	Proper solution
Access	Low (web-based applications)	Web-based VPN solution based on SSL VPN
	High (seamless network access)	Client-based VPN solution based on PPTP, L2TP, IPSec, or SSL VPNs
Security	Low (weak protocols)	Client-based VPN solution based on PPTP or L2TP VPNs
	High (strong protocols)	Client-based VPN solution based on IPSec or SSL VPNs
		Web-based VPN solution based on SSL VPN
Protocols support	Low (only TCP/IP)	Client-based VPN solution based on IPSec or SSL VPNs
		Web-based VPN solution based on SSL VPN
	High (TCP/IP, IPX/SPX, or NetBEUI)	Client-based VPN solution based on PPTP or L2TP VPNs
Cost	Low (web browser)	Web-based VPN solution based on SSL VPN
	High (client software)	Client-based VPN solution based on PPTP, L2TP, IPSec, or SSL VPNs

4.1.6 Remote Access VPN Formula

To extract remote access VPN logic Formula, we will refer to the remote access VPN solutions by the symbols shown in table (3) and to the remote access VPN requirements by the symbols shown in table (4).

Table (3) Remote Access VPN solutions Symbols

Remote Access VPN solutions	Symbol
Client-based VPN solution based on PPTP VPN	cPPTP
Client-based VPN solution based on L2TP VPN	cL2TP
Client-based VPN solution based on IPSec VPN	cIPSec

Client-based VPN solution based on SSL VPN	cSSL
Web-based VPN solution based on SSL VPN	wSSL
Client-based VPN solution based on PPTP/IPSec VPN	cPPTP/IPSec
Client-based VPN solution based on L2TP/IPSec VPN	cL2TP/IPSec

Table (4) Remote Access VPN requirements Symbols

requirement	Symbol	
Access	A	0 (Low - web-based applications)
		1 (High - seamless network access)
Security	S	0 (Low - weak protocols)
		1 (High - strong protocols)
Protocols Support	P	0 (Low - only TCP/IP)
		1 (High - TCP/IP, IPX/SPX, or NetBEUI)
Cost	C	0 (Low - web browser)
		1 (High - client software)

Tables (2), (3), and (4) are used to construct the following remote access VPN requirements logic equations:

$\text{Access} = A . (\text{cPPTP} + \text{cL2TP} + \text{cIPSec} + \text{cSSL}$
$+ \text{cPPTP/IPSec} + \text{cL2TP/IPSec}) + \overline{A} . (\text{wSSL})$ (1)

$\text{Security} = S . (\text{wSSL} + \text{cIPSec} + \text{cSSL} + \text{cPPTP/IPSec}$
$+ \text{cL2TP/IPSec}) + \overline{S} . (\text{cPPTP} + \text{cL2TP})$ (2)

$\text{Protocols} = P . (\text{cPPTP} + \text{cL2TP} + \text{cPPTP/IPSec}$
$+ \text{cL2TP/IPSec})$
$+ \overline{P} . (\text{wSSL} + \text{cIPSec} + \text{cSSL})$
(3)

$\text{Cost} = C . (\text{cPPTP} + \text{cL2TP} + \text{cIPSec} + \text{cSSL}$
$+ \text{cPPTP/IPSec} + \text{cL2TP/IPSec}) + \overline{C} . (\text{wSSL})$ (4)

By taking the common terms using intersection operation from (1) and (2) we get:

$AS = A . S . (\text{cIPSec} + \text{cSSL} + \text{cPPTP/IPSec}$
$+ \text{cL2TP/IPSec}) + A . \overline{S} . (\text{cPPTP} + \text{cL2TP})$
$+ \overline{A} . S . (\text{wSSL}) + \overline{A} . \overline{S} . (0)$ (5)

By taking the common terms using intersection operation from (5) and (3) we get:

$ASP = A . S . P . (\text{cPPTP/IPSec} + \text{cL2TP/IPSec})$
$+ A . S . \overline{P} . (\text{cIPSec} + \text{cSSL})$
$+ A . \overline{S} . P . (\text{cPPTP} + \text{cL2TP}) + A . \overline{S} . \overline{P} . (0)$
$+ \overline{A} . S . P . (0) + \overline{A} . S . \overline{P} . (\text{wSSL})$ (6)

By taking the common terms using intersection operation from (6) and (4) we get:

$ASPC = A . S . P . C . (\text{cPPTP/IPSec} + \text{cL2TP/IPSec})$
$+ A . S . P . \overline{C} . (0)$
$+ A . S . \overline{P} . C . (\text{cIPSec} + \text{cSSL})$
$+ A . S . \overline{P} . \overline{C} . (0)$
$+ A . \overline{S} . P . C . (\text{cPPTP} + \text{cL2TP})$
$+ A . \overline{S} . P . \overline{C} . (0) + \overline{A} . S . \overline{P} . C . (0)$
$+ \overline{A} . S . \overline{P} . C . (\text{wSSL})$ (7)

By rearranging the equation (7) we can get the following Proper remote access VPN logic formula:

Remote access VPN formula
$= \mathbf{A . S . P . C . (\text{cPPTP/IPSec} + \text{cL2TP/IPSec})}$
$+ \mathbf{A . S .} \overline{P} \mathbf{. C . (\text{cIPSec} + \text{cSSL})}$
$+ \mathbf{A .} \overline{S} \mathbf{. P . C . (\text{cPPTP} + \text{cL2TP})}$
$+ \overline{A} \mathbf{. S .} \overline{P} \mathbf{.} \overline{C} \mathbf{. (\text{wSSL})}$ **(8)**

4.2 Choosing Proper Site-to-Site VPN Solution

When providing site-to-site VPN solution, the web-based VPN solution which is based on SSL VPN should be ruled out. First of all, the web-based VPN solution is not seamless. When a web browser is used, simple tasks might be difficult and confusing to accomplish. Furthermore, the web- based solution offers limited access to applications.

4.2.1 Quality of Service (QoS) requirements

Secure VPN solution which is based on PPTP, L2TP, IPSec, or SSL VPNs is a good choice for site-to-site connections with low QoS requirements in which users need access to the non QoS applications such as e-mail, ftp, and http.

Trusted VPN solution which is based on MPLS VPN is a good choice for site-to-site connections with high QoS requirements in which users need access to the QoS applications such as voice over IP.

4.2.2 Topology requirements

Secure VPN solution which is based on PPTP, L2TP, IPSec, or SSL VPNs is a good choice for site-to-site connections with low topology requirements in which traffic flows follow a hub-and-spoke topology.

Trusted VPN solution which is based on MPLS VPN is a good choice for site-to-site connections with high topology requirements in which traffic flows follow a spoke-and-spoke topology (partial mesh topology or full mesh topology).

4.2.3 Security requirements

Trusted VPN solution which is based on MPLS VPN and Secure VPN solution which is based on PPTP or L2TP VPNs is a good choice for site-to-site connections with low security requirements, since the security of trusted VPN solution which is based on MPLS VPN depends on the separation of traffic and the secure VPN solution which is based on PPTP or L2TP uses weak authentication and encryption algorithms [2] [9].

Secure VPN solution which is based on IPSec or SSL VPNs is a good choice for site-to-site connections with high security requirements, where they are using strong authentication and encryption algorithms [2] [10].

4.2.4 Protocols support requirements

Secure VPN solution which is based on IPSec or SSL VPNs is a good choice for site-to-site connections with low protocols support requirements, where the only packets of TCP/IP network protocol are forwarded through the WAN.

Trusted VPN solution which is based on MPLS or Secure VPN solution which is based on PPTP or L2TP VPNs is a good choice for site-to-site connections with high protocols support requirements, where the packets of multiple network protocols such as TCP/IP, IPX/SPX, or NetBEUI are forwarded through the WAN.

4.2.5 Site-to-Site VPN Matrix

Table (5) shows the site-to-site VPN Matrix that is used to help enterprises for selecting the proper site-site VPN solution.

Table (5) Site-to-Site VPN Matrix

Requirements	Value		Proper solution
QoS	Low (best effort)		Secure VPN solution based on PPTP, L2TP, IPSec, or SSL VPNs
	High (class of service)		Trusted VPN solution based on MPLS VPN
Topology	Low (hup-and-spoke)		Secure VPN solution based on PPTP, L2TP, IPSec, or SSL VPNs
	High (spoke-and-spoke)		Trusted VPN solution based on MPLS VPN
Security	Low	(separation of traffic)	Trusted VPN solution based on MPLS VPN
		(weak protocols)	Secure VPN solution based on PPTP or L2TP VPNs
	High (strong protocols)		Secure VPN solution based on IPSec or SSL VPNs
Protocols support	Low (only TCP/IP)		Secure VPN solution based on IPSec or SSL VPNs
	High (TCP/IP, IPX/SPX, or NetBEUI)		Trusted VPN solution based on MPLS VPN
			Secure VPN solution based on PPTP or L2TP VPNs

4.2.6 Site-to-Site VPN Formula

To extract site-to-site VPN logic Formula, we will refer to the site-to-site VPN solutions by the symbols shown in table (6) and to the site-to-site VPN requirements by the symbols shown in table (7).

Table (6) Site-to Site VPN solutions Symbols

Site-to-Site VPN solutions	Symbol
Secure VPN solution based on PPTP VPN	sPPTP
Secure VPN solution based on L2TP VPN	sL2TP
Secure VPN solution based on IPSec VPN	sIPSec
Secure VPN solution based on SSL VPN	sSSL
Trusted VPN solution based on MPLS VPN	tMPLS
Secure VPN solution based on PPTP/IPSec VPN	sPPTP/IPSec
Secure VPN solution based on L2TP/IPSec VPN	sL2TP/IPSec
Hybrid VPN solution based on PPTP/MPLS VPN	hPPTP/MPLS
Hybrid VPN solution based on L2TP/MPLS VPN	hL2TP/MPLS
Hybrid VPN solution based on IPSec/MPLS VPN	hIPSec/MPLS
Hybrid VPN solution based on SSL/MPLS VPN	hSSL/MPLS
Hybrid VPN solution based on PPTP/IPSec/MPLS VPN	hPPTP/IPSec/MPLS
Hybrid VPN solution based on L2TP/IPSec/MPLS VPN	hL2TP/IPSec/MPLS

Table (7) Site-to-Site VPN requirements Symbols

Requirement	Symbol	
QoS	Q	0 (Low – best effort)
		1 (High – class of service)
Topology	T	0 (Low – hup-and-spoke)
		0 (High – Spoke-and-spoke)
Security	S	0 (Low – separation of traffic or weak protocols)
		1 (High - strong protocols)
Protocols Support	P	0 (Low - only TCP/IP)
		1 (High - TCP/IP, IPX/SPX, or NetBEUI)

Tables (5), (6), and (7) are used to construct the following site-to-site VPN requirements logic equations:

$$\begin{aligned}\text{QoS} = \text{Q} \,.\, (\, &\text{tMPLS} + \text{hPPTP/MPLS} + \text{hL2TP/MPLS} \\ &+ \text{hIPSec/MPLS} + \text{hSSL/MPLS} + \text{hPPTP/IPSec/MPLS} \\ &+ \text{hL2TP/IPSec/MPLS}\,) + \overline{\text{Q}} \,.\, (\, \text{sPPTP} + \text{sL2TP} \\ &+ \text{sIPSec} + \text{sSSL} + \text{sPPTP/IPSec} + \text{sL2TP/IPSec}\,) \qquad (9)\end{aligned}$$

$$\begin{aligned}\text{Topology} = \text{T} \,.\, (\, &\text{tMPLS} + \text{hPPTP/MPLS} + \text{hL2TP/MPLS} \\ &+ \text{hIPSec/MPLS} + \text{hSSL/MPLS} \\ &+ \text{hPPTP/IPSec/MPLS} + \text{hL2TP/IPSec/MPLS}\,)\end{aligned}$$

$$\begin{aligned}&+\overline{T}\,.\,(\,\text{sPPTP} + \text{sL2TP} + \text{sIPSec} + \text{sSSL}\\&+ \text{sPPTP/IPSec} + \text{sL2TP/IPSec}\,) \qquad (10)\end{aligned}$$

$$\begin{aligned}\text{Security} = {}& S\,.\,(\,\text{sIPSec} + \text{sSSL} + \text{sPPTP/IPSec}\\&+ \text{sL2TP/IPSec} + \text{hIPSec/MPLS}\\&+ \text{hSSL/MPLS} + \text{hPPTP/IPSec/MPLS}\\&+ \text{hL2TP/IPSec/MPLS})\\&+\overline{S}\,.\,(\,\text{sPPTP} + \text{sL2TP} + \text{tMPLS}\\&+ \text{hPPTP/MPLS} + \text{hL2TP/MPLS}\,) \qquad (11)\end{aligned}$$

$$\begin{aligned}\text{Protocols} = {}& P\,.\,(\,\text{sPPTP} + \text{sL2TP} + \text{sPPTP/IPSec}\\&+ \text{sL2TP/IPSec} + \text{tMPLS} + \text{hPPTP/MPLS}\\&+ \text{hL2TP/MPLS} + \text{hPPTP/IPSec/MPLS}\\&+ \text{hL2TP/IPSec/MPLS}\,) + \overline{P}\,.\,(\,\text{sIPSec} + \text{sSSL}\\&+ \text{hIPSec/MPLS} + \text{hSSL/MPLS}\,) \qquad (12)\end{aligned}$$

By taking the common terms using intersection operation from (9) and (10) we get:

$$\begin{aligned}QT = {}& Q.\,T\,.\,(\,\text{tMPLS} + \text{hPPTP/MPLS} + \text{hL2TP/MPLS}\\&+ \text{hIPSec/MPLS} + \text{hSSL/MPLS} + \text{hPPTP/IPSec/MPLS}\\&+ \text{hL2TP/IPSec/MPLS}\,) + Q.\,\overline{T}\,.\,(\,0\,) + \overline{Q}\,.\,T\,(\,0\,)\\&+\overline{Q}\,.\,\overline{T}\,.\,(\text{sPPTP} + \text{sL2TP} + \text{sIPSec} + \text{sSSL}\\&+ \text{sPPTP/IPSec} + \text{sL2TP/IPSec}\,) \qquad (13)\end{aligned}$$

By taking the common terms using intersection operation from (13) and (11) we get:

$$\begin{aligned}QTS = {}& Q.\,T\,.\,S\,.\,(\,\text{hIPSec/MPLS} + \text{hSSL/MPLS}\\&+ \text{hPPTP/IPSec/MPLS} + \text{hL2TP/IPSec/MPLS}\,)\\&+ Q\,.\,T\,.\overline{S}\,.\,(\,\text{tMPLS} + \text{hPPTP/MPLS} + \text{hL2TP/MPLS}\,)\\&+\overline{Q}\,.\,\overline{T}\,.\,S\,.\,(\,\text{sIPSec} + \text{sSSL} + \text{sPPTP/IPSec}\\&+ \text{sL2TP/IPSec}\,) + \overline{Q}\,.\,\overline{T}\,.\,\overline{S}\,.\,(\,\text{sPPTP} + \text{sL2TP}\,) \qquad (14)\end{aligned}$$

By taking the common terms using intersection operation from (14) and (12) we get:

$$\begin{aligned}QTSP = {}& Q.\,T\,.\,S\,.\,P\,.\,(\,\text{hPPTP/IPSec/MPLS}\\&+ \text{hL2TP/IPSec/MPLS})\\&+ Q.\,T\,.\,S\,.\,\overline{P}\,.\,(\,\text{hIPSec/MPLS} + \text{hSSL/MPLS}\,)\\&+ Q\,.\,T\,.\,\overline{S}\,.\,P\,.\,(\,\text{tMPLS} + \text{hPPTP/MPLS}\\&+ \text{hL2TP/MPLS}) + Q\,.\,T\,.\,\overline{S}\,.\,\overline{P}\,.\,(\,0\,)\\&+\overline{Q}\,.\,\overline{T}\,.\,S\,.\,P\,.\,(\,\text{sPPTP/IPSec} + \text{sL2TP/IPSec}\,)\\&+\overline{Q}\,.\,\overline{T}\,.\,S\,.\,\overline{P}\,.\,(\,\text{sIPSec} + \text{sSSL}\,)\\&+\overline{Q}\,.\,\overline{T}\,.\,\overline{S}\,.\,P\,.\,(\text{sPPTP} + \text{sL2TP}\,)\\&+\overline{Q}\,.\,\overline{T}\,.\,\overline{S}\,.\,\overline{P}\,.\,(\,0\,) \qquad (15)\end{aligned}$$

By rearranging the equation (15) we can get the following Proper site-to-site VPN solution logic equation :

Site-to-site VPN formula

$$\begin{aligned}&\mathbf{= Q\,.\,T\,.\,S\,.\,P\,.\,(\,\text{hPPTP/IPSec/MPLS}}\\&\mathbf{+\,\text{hL2TP/IPSec/MPLS}\,)}\\&\mathbf{+\,Q\,.\,T\,.\,S\,.\,\overline{P}\,.\,(\,\text{hIPSec/MPLS} + \text{hSSL/MPLS}\,)}\\&\mathbf{+\,Q\,.\,T\,.\,\overline{S}\,.\,P\,.\,(\,\text{tMPLS} + \text{hPPTP/MPLS}}\\&\mathbf{+\,\text{hL2TP/MPLS}\,)}\\&\mathbf{+\,\overline{Q}.\overline{T}.\,S\,.\,P\,.\,(\,\text{sPPTP/IPSec} + \text{sL2TP/IPSec}\,)}\\&\mathbf{+\,\overline{Q}.\overline{T}.\,S\,.\,\overline{P}\,.\,(\,\text{sIPSec} + \text{sSSL}\,)}\\&\mathbf{+\,\overline{Q}.\overline{T}.\overline{S}.\,P\,.\,(\,\text{sPPTP} + \text{sL2TP}\,)} \qquad \mathbf{(16)}\end{aligned}$$

5. Conclusion and Future Work

Creating a WAN with VPN technology might not be as simple as it sounds. There are many different VPN solutions out there, and just deciding which one to choose can be difficult since they all have advantages and disadvantages. VPN solutions can be categorized as Secure or Trusted VPNs, Client-based or Web-based VPNs , Customer Edge-based or Provider Edge-based VPNs , or Outsourced or In-house VPNs . These categories often overlap each other. This paper has proposed the remote access VPN formula that depends on remote access connections requirements (access, security, protocols support, and cost) and remote access VPN solutions (client-based VPNs and web-based VPNs). This paper also has proposed the site-to-site VPN formula that depends on site-to-site connections requirements (QoS, topology, security, and protocols support) and site-to-site VPN solutions (secure VPNs, trusted VPNs, and hybrid VPNs).

This paper has proposed the proper VPN solution that will be used to serve as a basis when creating an enterprise WAN which connects sites and users together using VPN technology, but it is not practically to implement this proposal on the real Internet. So the further work for this paper is building this solution for an enterprise that want to use such of those solutions, or simulate these solutions on the Internet.

References

[1] R. Fisli, “Secure Corporate Communications over VPN-Based WANs,” Master’s Thesis in Computer Science at the School of Computer Science and engineering, Royal Institute of Technology, sweden, 2005.

[2] J. C. Snader, “VPNs ILLUSTRATED: Tunnels, VPNs, and IPSec,” Addison-Wesley, 2006.

[3] K.n Hamzeh, G. S. Pall, W. Verhein, J. Taarud, W. A. Little, and G. Zorn, “Point to Point Tunneling Protocol (PPTP),” IETF RFC 2637, July 1999.

[4] W. Townsley, A. J. Valencia, A. Rubens, G. S. Pall, G. Zorn, and B. Palter, “Layer Two Tunneling Protocol (L2TP),” IETF RFC 2661, August 1999.

[5] IETF RFCs 2401-2411, and 2451, “IPSec,” 1999.

[6] O. Freier, P. Karlton, and P. C. Kocker, “ The SSL Protocol: Version 3.0,” IETF RFC draft-freier-ssl-version3-02, November 1996.

[7] E. C. Rosen, Y. Rekhter, “BGP/MPLS VPNs,” IETF RFC 2547, March 1999.

[8] VPN Consortium home page, www.vpnc.org.

[9] Schneier, and Mudge, “Cryptanalysis of Microsoft’s Point-to-Point Tunneling Protocol (PPTP),” Proceeding of the 5th ACM Conference on Communication and Computer Security, pp. 132-141 ACM Press, 1998.

[10] Wanger, and Schneier, “Analysis of the SSL 3.0 protocol,” The Second USENIX Workshop on Electronic Commerce Proceedings, pp. 29-40, 1996.