

**Project Report  
ECE 646 (Fall 2001)**

**Comparison of VPN Protocols – IPsec, PPTP, and L2TP**

**Poonam Arora, Prem R. Vemuganti, Praveen Allani**

**Department of Electrical and Computer Engineering  
George Mason University  
Fairfax, VA 22202**



## Table of Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>6</b>
1.1	WHAT IS VIRTUAL PRIVATE NETWORK (VPN)?.....	6
1.2	WHY VPNS ARE SO POPULAR TODAY? .....	7
1.3	TYPES OF VPN SERVICES .....	8
1.3.1	LAN Interconnect VPN.....	8
1.3.2	Dial-up VPN Services.....	8
1.3.3	Extranet VPN Services.....	9
<b>2</b>	<b>OVERVIEW OF TUNNELING .....</b>	<b>11</b>
2.1	TUNNELING TECHNOLOGIES.....	11
2.2	HOW TUNNELING WORKS FOR DIFFERENT PROTOCOLS? .....	12
2.3	TUNNELING PROTOCOLS AND REQUIREMENTS.....	12
<b>3</b>	<b>IP SECURITY ARCHITECTURE.....</b>	<b>13</b>
3.1	SECURITY ASSOCIATIONS .....	13
3.2	SECURITY DATABASES .....	15
3.2.1	Security Policy Database.....	15
3.2.2	Security Association Database .....	15
3.3	AUTHENTICATION HEADER .....	15
3.4	ENCAPSULATING SECURITY PAYLOAD.....	18
3.5	INTERNET KEY EXCHANGE.....	21
3.5.1	ISAKMP.....	21
3.5.2	Oakley.....	22
3.5.3	SKEME .....	23
<b>4</b>	<b>PPTP.....</b>	<b>24</b>
4.1	TUNNELING IN PPTP.....	24
4.2	TYPES OF TUNNELING:.....	25
4.2.1	Compulsory Tunneling.....	25
4.2.2	Voluntary Tunneling.....	25
4.3	MICROSOFT PPTP.....	26
4.3.1	Authentication in PPTP .....	27
4.3.2	Encryption in PPTP.....	27
<b>5</b>	<b>LAYER 2 TUNNELING PROTOCOL (L2TP).....</b>	<b>29</b>
5.1	TYPES OF TUNNELING .....	29
5.1.1	Compulsory Tunneling.....	29
5.1.2	Voluntary Tunneling.....	30
5.2	HOW DOES IT WORK? .....	31
5.3	L2TP PROTOCOL CHARACTERISTICS .....	31
5.4	L2TP OVER SPECIFIC MEDIA .....	32
5.5	L2TP SECURITY CONSIDERATIONS.....	32
5.6	L2TP WITH IPSEC.....	33
<b>6</b>	<b>COMPARISON OF PROTOCOLS .....</b>	<b>35</b>
6.1	SECURITY.....	35
6.1.1	Authentication.....	35
6.1.2	Integrity.....	35
6.1.3	Confidentiality .....	36
6.1.4	Key Management .....	36
6.1.5	Attacks on VPN.....	36
6.2	PERFORMANCE .....	40

<b>6.3</b>	<b>SCALABILITY .....</b>	<b>41</b>
<b>6.4</b>	<b>FLEXIBILITY .....</b>	<b>41</b>
<b>6.5</b>	<b>INTEROPERABILITY .....</b>	<b>41</b>
<b>6.6</b>	<b>MULTIPROTOCOL SUPPORT .....</b>	<b>42</b>
<b>6.7</b>	<b>APPLICATIONS .....</b>	<b>42</b>
<b>7</b>	<b>VENDORS .....</b>	<b>43</b>
<b>8</b>	<b>CONCLUSION.....</b>	<b>44</b>
	<b>REFERENCES .....</b>	<b>45</b>

## List of Figures

FIGURE 1 VIRTUAL PRIVATE NETWORK CONNECTION .....	6
FIGURE 2 LAN INTERCONNECT.....	8
FIGURE 3 DIAL-UP VPN SERVICES .....	9
FIGURE 4 EXTRANET VPN SERVICE.....	10
FIGURE 5 TUNNELING TECHNIQUE .....	11
FIGURE 6 TRANSPORT AND TUNNEL MODES .....	14
FIGURE 7 THE AUTHENTICATION HEADER (AH) FORMAT.....	16
FIGURE 8 AH TRANSPORT MODE .....	16
FIGURE 9 AH TUNNEL MODE .....	17
FIGURE 10 ESP HEADER, TRAILER, AND AUTHENTICATION SEGMENT FORMATS .....	18
FIGURE 11 THE ENCAPSULATING SECURITY PAYLOAD (ESP) FORMAT .....	19
FIGURE 12 ESP TRANSPORT MODE .....	20
FIGURE 13 ESP TUNNEL MODE .....	20
FIGURE 14 ISAKMP MESSAGE FORMAT.....	22
FIGURE 16 STRUCTURE OF A PPTP PACKET CONTAINING USER DATA .....	25
FIGURE 17 PPTP CONTROL CONNECTION PACKET .....	26
FIGURE 18 PPTP TUNNELED DATA .....	26
FIGURE 19 COMPULSORY TUNNELING EXAMPLE .....	30
FIGURE 20 VOLUNTARY TUNNELING EXAMPLE .....	30
FIGURE 21 REMOTE USER DIAL-IN USING L2TP .....	31
FIGURE 22 L2TP ENCRYPTED CONTROL MESSAGE.....	34
FIGURE 23 L2TP TUNNELING PROCESS .....	34

[Click here to download full PDF material](#)