

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
ELEKTROTEHNIČKI FAKULTET

SVEUČILIŠNI STUDIJ

KOMPARATIVNA ANALIZA VPN PROTOKOLA
TUNELIRANJA

Diplomski rad

Perica Pejić

Osijek, 2014.

Sadržaj

1. UVOD	5
1.1. Zadatak diplomskog rada.....	5
2. VPN – OPĆI PREGLED	6
2.1. Vrste VPN rješenja	7
2.2. Tuneliranje.....	9
2.3. Sigurnost podataka u VPN-u	11
3. VPN PROTOKOLI TUNELIRANJA.....	14
3.1. IPsec.....	14
3.1.1. Autentifikacijsko zaglavlje (AH)	15
3.1.2. ESP protokol	16
3.1.3. Sigurnosne asocijacije (SA)	18
3.1.4. Tunelirajući i prijenosni način rada.....	20
3.2. PPTP.....	22
3.3. L2TP	23
3.3.1. Dobrovoljno i obvezno tuneliranje.....	26
3.3.2. L2TP/IPsec	27
3.4. SSTP.....	28
3.4.1. SSL.....	30
3.5. Usporedba protokola.....	31
4. OPIS I RJEŠENJE PROBLEMA	35
4.1. Opis problema.....	35
4.2. Odabir sustava za rješavanje problema	35
4.3. Odabir i postavljanje klijentskog računala	35
4.3.1. Stvaranje VPN veze	35
4.3.2. Postavljanje PPTP protokola.....	37
4.3.3. Postavljanje L2TP/IPsec protokola	39

4.3.4.	Postavljanje SSTP protokola.....	40
4.4.	Odabir i postavljanje poslužitelja	40
4.4.1.	Postavljanje VPN poslužitelja.....	41
4.4.2.	Stvaranje korisnika	44
4.4.3.	Izdavanje certifikata	45
4.4.4.	Postavljanje unaprijed dijeljenog ključa	48
4.5.	Odabir i postavljanje testne računalne mreže	49
4.6.	Mjerenje i rezultati mjerenja.....	51
4.7.	Analiza rezultata mjerenja	51
5.	ZAKLJUČAK	53
	LITERATURA.....	54
	SAŽETAK.....	56
	ABSTRACT	56
	ŽIVOTOPIS	57

SAŽETAK

U radu je glavni zadatak bio analizirati VPN protokole tuneliranja, te na primjeru opisati proces implementacije različitih protokola tuneliranja. Objašnjene su virtualne privatne mreže, različiti protokoli tuneliranja koji se koriste za uspostavljanje virtualnih privatnih mreža, te je opisan postupak postavljanja VPN poslužitelja i VPN klijenta za korištenje različitih protokola tuneliranja. Za prikaz procesa uspostavljanja virtualne privatne mreže je odabran karakterističan scenarij VPN udaljenog pristupa. Pritom su za kao VPN klijent i VPN poslužitelj korištena računala s Windows operativnim sustavima, koji imaju ugrađeno VPN rješenje koje omogućuje korištenje nekoliko različitih protokola tuneliranja.

Ključne riječi: virtualne privatne mreže, PPTP, L2TP, IPsec, SSTP, udaljeni pristup.

ABSTRACT

The paper's main task was to analyze the VPN tunneling protocols, and describe on example the process of implementation of the various tunneling protocols. Paper explains virtual private network, different tunneling protocols used to establish virtual private networks, and describes the procedure for setting up a VPN server and VPN client to use different tunneling protocols. For describing the process of establishing a virtual private network typical remote access scenario VPN is selected. For VPN client and the VPN server computers with Windows operating systems are used, which have built-in VPN solution that makes use of several different tunneling protocols.

Key words: virtual private network, PPTP, L2TP, IPsec, SSTP, remote access.