

Sadržaj:

UVOD	3
1. Pojam virtuelnih privatnih mreža	5
1.1. Šta predstavljaju virtuelne privatne mreže?	6
1.2. Prednosti virtuelnih privatnih mreža	6
1.3. Ciljevi realizacije virtuelnih privatnih mreža	6
1.4. Izbor prave virtuelne privatne mreže	7
2. Osnovna načela zaštite podataka	9
2.1. Model zaštite informacija	9
2.1.1. Osobine zaštite informacija	9
2.1.2. Stanja informacije	10
2.1.2.1. Zaštita odbačenih medija i prikazanih (output) podataka	11
2.1.3. Mjere sigurnosti	12
2.1.4. Model zaštite informacija	12
2.2. Još neki pojmovi o sigurnosti podataka	13
3. Šifriranje podataka štiti povjerljivost	16
3.1. Osnovni pojmovi kriptografije	16
3.2. Simetrični kriptosistemi	18
3.2.1. Supstitucijske šifre	19
3.2.2. Transpozicijske šifre	19
3.2.3. Jednokratna bilježnica	19
3.3. Uređaji za šifriranje	20
3.4. DES - Data Encryption Standard	22
3.4.1. Historija DES-a	22
3.4.2. Svojstva DES-a	22
3.4.3. Kriptoanaliza DES-a	23
3.5. Još neki moderni blokovni kriptosistemi	23
3.5.1. IDEA	23
3.5.2. CAST-128	24
3.5.3. RC5	24
3.6. AES - Advanced Encryption Standard	24
4. Provjera integriteta i autentičnosti	28
4.1. Ideja javnog ključa	28
4.1.1. Kriptosistem s javnim ključem vs. simetrični kriptosistem	29
4.2. RSA kriptosistem	30
4.2.1. Kriptoanaliza RSA kriptosistema	30
4.3. Jednosmjerne (Hash) funkcije	31
4.3.1. MD5	32
4.3.2. SHA	32
4.3.2.1. Primjer primjene hash funkcije	33
4.4. Digitalni potpisi	33
4.4.1. Osobine digitalnog potpisa	34

4.5.	Digitalni certifikati	35
4.5.1.	Sadržaj digitalnog potpisa	35
4.6.	Certificate Authorities - uprava za certifikate	37
5.	Protokoli virtuelnih privatnih mreža	38
5.1.	Protokoli i tuneliranje	38
5.2.	PPTP	41
5.3.	L2TP	42
5.4.	IPSec	42
5.4.1.	Dizajn sistema	43
5.4.2.	Osnovni protokoli	43
5.4.2.1.	Authentication Header (AH) protokol	43
5.4.2.2.	Encapsulated Security Payload (ESP) protokol	43
5.4.2.3.	IKE protokol	43
5.4.3.	Obrada paketa	44
5.4.3.1.	Obrada ulaznih paketa	44
5.4.3.2.	Obrada izlaznih paketa	44
5.4.4.	Implementacije IPsec protokola	44
5.5.	Dostupnost i performanse	45
5.5.1.	Šta je QoS?	45
5.5.2.	Pristupi osiguranju kvalitete usluge	46
5.5.2.1.	IntServ	46
5.5.2.2.	DifferServ	46
6.	VPN - rješenje za sigurno umrežavanje udaljenih lokacija	50
6.1.	Opis situacije	49
6.2.	Da li postoji optimalno VPN rješenje?	50
6.3.	Smjernice za odabir VPN rješenja	50
6.4.	Potrebe za sigurnim umrežavanjem udaljenih lokacija	51
6.4.1.	Scenarij 1: Osnovno povezivanje filijale	51
6.4.2.	Scenarij 2: Osnovno povezivanje posla s poslom	52
6.4.3.	Scenarij 3: Zaštita L2TP dobrovoljnog tunela s IPsec-om	53
6.4.4.	Scenarij 4: Sigurni i predvidljivi rezultati (VPN i QoS)	55
7.	ZAKLJUČAK	57
8.	NOMENKLATURE	58
9.	Literatura	60