Remote Access VPN

Meszlényi Zoltán
Borús András
SZTE ESZK
2009. 11. 10.

I. Bevezetés

Szélessávú Internet otthoni munka céljára: KTV és ADSL
Keretszerződés a szolgáltatókkal

Előny:

- Egyetemi IP címek.
- Egyetemi menedzselés.

Hátrány:

- Egyedi rendszerek.
- A keretszerződés rugalmatlan.

Megoldás: Lakossági csomagok + Remote Access VPN
+ self-signed tanúsítványok

II. Cisco EzVPN vs OpenVPN

1. Összehasonlítás/1

	Cisco EzVPN	**OpenVPN**
Technológia	IPSec	SSL
Protokoll	ESP+UDP+TCP	TCP vagy UDP
Kiszolgáló hardver	7301/SA-VAM2, 6500/Sup720/ SPA	PC

1. Összehasonlítás/2

	Cisco EzVPN	**OpenVPN**
Kiszolgáló szoftver	IOS	Linux+OpenVPN
Kliens szoftver	Cisco VPN Client, Anyconnect (lesz)	OpenVPN kliens

1. Összehasonlítás/3

	Cisco EzVPN	**OpenVPN**
Támogatott kliens op. rendszerek	Windows 98, ME, NT4, 2000, XP, Vista, Linux, Mac OS X, Solaris	2000, XP, Vista, Linux, OpenBSD, FreeBSD, NetBSD, Mac OS X, Solaris
64 bites op. rendszer támogatás	nincs (lesz)	van

1. Összehasonlítás/4

	Cisco EzVPN	**OpenVPN**
Ár	drága	olcsó
Support	pénzes	ingyenes
Forráskód	zárt	nyílt
Skálázhatóság	nincs	van
Egyéb előnyök	• Megvannak az eszközök	• Vmware támogatás •Ethernet tunnel

2. Cisco EzVPN problémák/1

- Még nincs 64 bites kliens.
- Ethernet tunnelt nem tud (GRE vagy L2TPv3 kell).
- A kliens szoftver COCOM listás.
- A 6500-ason kulcscserénél reautentikációt kér, a kulcscsere nélküli működés max 19 óra.

2. Cisco EzVPN problémák/2

- NAT problémák:
  - Az IPSec protokollcsomagot (IKE+ESP) nem tudja kezelni a NAT/PAT. Emiatt kifejlesztették a NAT-Traversalt, ami UDP-be „csomagolja” az IPSec-et. A NAT-T 4500-as porton működik, ezt nem lehet változtatni. Az UDP-be csomagolás nem jelent megoldást olyan helyeken, ahol tűzfalazva van a kimenő UDP forgalom.
  - A Cisco megalkotta a cTCP protokollt. A cTCP, TCP protokollba „csomagolja” az IPSec-et. A portszám szabadon változtatható. A 7301-es router 12.4(9)T-s IOS verziótól támogatja a cTCP-t, a 6500/Sup720/SPA nem.

3. OpenVPN problémák

- Windows 2000 előtti MS op. rendszerek nem támogatottak.
- Venni kell hardvert.

III. Vastag vagy vékony VPN kliens?

- **Vastag kliens (client-based)**
  - Előny:
    - Teljes protokoll stack.
  - Hátrány:
    - Speciális kliens szoftverre van szükség.
    - A telepítéshez rendszergazdai jogok kellenek.
- **Vékony kliens (clientless)**
  - Előny:
    - Nem kell kliens szoftver, elég egy böngésző.
  - Hátrány:
    - Részleges protokoll stack, gyakorlatilag http(s).

IV. Hardver

DELL PowerEdge R710 (2 db):

- 2xE5530 CPU (2.4 GHz, quad core)
- 6x2 Gbyte RAM
- 2x750 Gbyte SAS diszk
- 6x1 Gbps Ethernet