Fábián Zoltán – Hálózatok elmélet

OpenVPN – ingyenes alternatíva

Mikor és miért használjuk?

- Windows NT / XP / 2003 / Vista / Win7 /2008 támogatja
- Linux minden disztribúcióját támogatja
- Beágyazott (embedded) rendszerekben is használják (Hardver eszközben, Linux alapú op. rendszer)

- Multiplatformos környezetben
  - Linux szerver / tűzfal, vegyesen Windows és Linux kliensek
  - Windows szerver, és vegyesen Windows és Linux kliensek
  - Windows munkaállomáshoz más Windows munkaállomásokkal szeretnénk VPN-nel kapcsolódni

- Jól dokumentált, rengeteg leírás található hozzá a Neten

OpenVPN beüzemelése Windowson

- A szerver és a kliens ugyanaz a szoftver, csak a konfiguráció változik
- Letöltés: http://openvpn.net/index.php/open-source/downloads.html
- Vista / Windows 7 / Windows 2008 Server esetén csak az OpenVPN 2.1.1 vagy újabb változat megfelelő!

A telepítés lépései

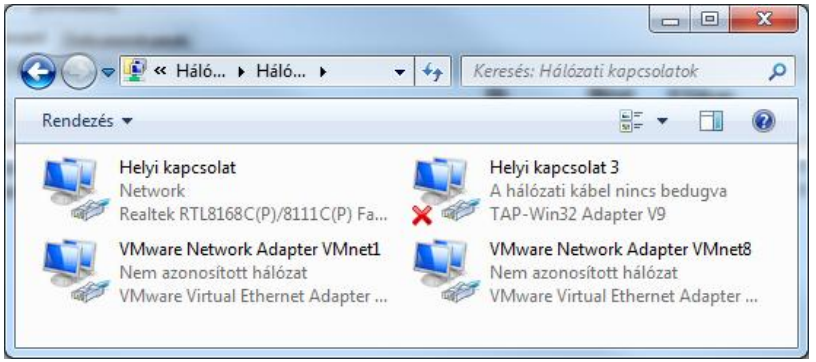
- Varázsló indítása
- Licenc elfogadása
- Milyen komponensek települjenek (minden)
- A telepítés helye:
  - Vista / Win 7 /Win2008 : C:\Program Files (x86)\OpenVPN
  - Win XP: C:\Program Files\OpenVPN

Driver feltelepül

- Windows Vista / 2008 / Windows 7 esetén V9 adapter jó csak!

Telepítés után az OpenVPN könyvtárban

- \Bin – A telepített alkalmazások
- \Driver – az új virtuális hálózati csatoló fájljai
  TAP-Win32 adapter V9
- \config – Konfigurációs állományok helye
  - Az itt található konfigurációs állományok hozzák létre a kapcsolat paramétereit
- \easy-rsa – a kulcskészítéshez szükséges könyvtár
- \log – A csatlakozások naplófájljai
- \sample-config – minta fájl



- Létrejön egy ikon a Desktopon
  => GUI indítóikonja

A kapcsolat létrehozásának lépései

- Kulcsgenerálás a VPN szerveren
  - A szerver részére
  - A kliensek részére
    Az \easy-rsa-ban található fájlok segítségével
- Tűzfalak konfigurálása szerver és | vagy kliens oldalon
- Konfiguráció beállítása a szerveren
  Egy db. Konfigurációs fájl beállítása
- Konfiguráció beállítása a kliensen
  - Ahány majdani kliens, annyi konfigurációs állomány – de abban csak néhány adat különbözik

Kulcsgenerálás

- c:\Program Files (x86)\OpenVPN\easy-rsa\

Vars.bat - alapértelmezett értékek beállítása
build-ca.bat – Certificate előállítása
build-dh.bat – Diffi-Hellman paraméterek előállítása
build-key-server.bat – Szerver kulcs előállítása
build-key.bat dellzoli – Kliens kulcs előállítása

- A fenti parancsokat érdemes egy batch fájlba szervezni.

Clean-all.bat - Ha a fenti kulcsok generálása során hibát vétünk, ezzel törölhetjük az addigi tevékenységet

A kulcsok kiosztása

- A kulcsok a szerveren jönnek létre és ott tárolódnak egy adatbázisban a \easy-rsa\keys könyvtárban
- A kulcsokat el kell juttatni a klienshez
- Egy kulccsal egy időben egy kliens kapcsolódhat a szerverhez
- Nem szükséges usernév, password beállítása
- A kliens kulcsait a szerveren lévő kulcs fogja aláírni – hitelesíteni!

Példa egy kulcsra: CA.CRT

- -----BEGIN CERTIFICATE-----
  MIIDTDCCArWgAwIBAgIJAJkx5UoFngqCMA0GCSqGSIb3DQEBBQUAMHgxCzAJBgNVBAYTAkh
  VMQswCQYDVQQIEwJCUDERMA8GA1UEBxMIQnVkYXBlc3QxDzANBgNVBAoTBlBldHJpazEQ
  MA4GA1UEAxMHcGZTZW5zZTEmMCQGCSqGSIb3DQEJARYXZmFiaWFuLnpvbHRhbkBwZXRy
  aWsuaHUwHhcNMTxxxxxxxxxxxAxMDI4MjAyOTE2WhcNMjAxMDI1MjAyOTE2WjB4MQswCQY
  DVQQGEwJlVTELMAkGA1UECBMCQlAxETAPBgNVBAcTCEJ1ZGFwZXN0MQ8wDQYDVQQKE
  wZQZXRyaWsxEDAOBgNVBAMTB3BmU2Vuc2UxJjAkBgkqhkiG9w0BCQEWF2ZhYmlhbi56b2x0
  YW5AcGV0cmlrLmh1MIGfMA0GCSqGSxxxxxxxxxxQUAA4GNADCBiQKBgQCZA3CCSnwgmgV8
  d+rLiuuFGcg+F/fwT+SpmgRxZfOvO7XW9gg6X1pg8ds95f28fBkTNwAGjIyeVI6hwGhaszRCtMNRl
  kfXIZZF0oroSN4UFfHz1NZccZ/4W1/t6Kah3BxDCHtqCXoKxmaxp9hIa11Fzalls8nBdTqJfZnMQlPG
  4QIDAQABo4HdMIHaMB0GA1UdDgQWBBShsm62dO+gu2msls79b+Lwz0rCVjCBqgYDVR0jBIGi
  MIGfgBShsm62dO+gu2msls79b+Lwz0rCVqF8pHoweDELMAkGA1UEBhMCSFUxCzAJBgNVBAgT
  AkJQMREwDwYDVQQHEwhCdWRhcGVzdDEPMA0GA1UEChMGUGV0cmlrMRAwDgYDVQQDE
  wdwZlNlbnNlMSYwJAYJKoZIhvcNAQkuQHBldHJpay5odYIJAJkx5UoFngqCMAwGA1UdEwQFMA
  MBAf8wDQYJKoZIhvcNAQEFBQADgYEAOgKLw8gny19cxtoXZm10QuPm6ZNe3TpF8mG+6Cc1
  CnUyPMq9G6MNLqzUkOFTAqbuqblgP601tjDVCmjBfbGn/yzfJAkEEF/NuThEtbHUSgUFKAmAa
  w9oaeB/RNwQgPh6r51wYmk+mkcmsuU5/t6TBTYkkL/hWfbGOlhzfVgajtE=hiujhzgghfhgfgfdgfdf
  -----END CERTIFICATE-----

- Ez a kulcs fogja a szerveren aláírni a többi generált kulcsot!

Példa a kliens certificate-re

- ----BEGIN CERTIFICATE----
MIIDXzCCAsigAwIBAgIBAjANBgkqhkiG9w0BAQQFADB4MQswCQYDVQQGEwJlVTELMAkGA1
UECBMCQlAxETAPBgNVBAcTCEJ1ZGFwZXN0MQ8wDQYDVQQKEwZQZXRyaWsxEDAOBgNV
BAMTB3BmU2Vuc2UxJjAkBgkqhkiG9w0BCQEWF2ZhYmlhbi56b2x0YW5AcGV0cmlrLmh1MB4X
DTEwMTAyODIwMzA1MFoXDTIwMTAyNTIwMzA1MFowZjELMAkGA1UEBhMCSFUxCzAJBgNV
BAgTAkJQMQ8wDQYDVQQKEwZQZXRyaWsxETAPBgNVBAMTCGRlbGx6b2xpMSYwJAYJKoZI
hvcNAQkBFhdmYWJpYW4uem9sdGFuQHBldHJpay5odTCBnzANBgkqhkiG9w0BAQEFAAOBjQA
wgYkCgYEAqVFm32EbshIX/+mnS05EGKzCGaOK+R609w5RPA5tGzZeawJfGnB1QU9SFFsFMAu
YibV99ugRGp0/mmV+PxHCWlTT2IfkXG699aVv+hsrN8EVGiHQN1TQ1ip5rAbgigV8nwhGVDw28
D069IzezDrLWFXS+jdPjYji6k5VU2ByAYkCAwEAAaOCAQkwggEFMAkGA1UdEwQCMAAwLAYJY
IZIAYb4QgENBB8WHU9wZW5TU0wgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1UdDgQWBBR
zm21W+YPe9DM5V0bMuRL+rQp9DjCBqgYDVR0jBIGiMIGfgBShsm62dO+gu2msls79b+Lwz0rCV
qF8pHoweDELMAkGA1UEBhMCSFUxCzAJBgNVBAgTAkJQMREwDwYDVQQHEwhCdWRhcGVz
dDEPMA0GA1UEChMGUGV0cmlrMRAwDgYDVQQDEwdwZlNlbnNlMSYwJAYJKoZIhvcNAQkBF
hdmYWJpYW4uem9sdGFuQHBldHJpay5odYIJAJkx5UoFngqCMA0GCSqGSIb3DQEBBAUAA4GB
AHMRBn3jmOjaqmF4A8K0ygPpt7hKhdd+JrhMCpDgAENyR1y1Q0k1abuBKB0TgwCdrPOg7hPJR
gI+a6Wg4h+se2DVMi0Z8unXuM6fnH+ljKfobItFVujZGDz+i+wcT7A0WPXSQAqq578RFNpI6yDSO
-----END CERTIFICATE-----

Példa a kliens kulcsra

- -----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQCpUWbfYRuyEhf/6adLTkQYrMIZo4r5HrT3DlE8Dm0
bNl5rAl8acHVBT1lUWwUwC5iJtX326BEanT+aZX4/EcJaVNPYh+Rcbr31p
W/6Gys3wRUaIdA3VNDWKnmsBuCKBXyfCEZUPDbwPTr0jN7MOstYVd
L6N0+NiOLqTlVTYHlBiQIDAQABAoGAARu8TaglE2FU8OLpqm+HuJWg
66QLa9gMnTVlyLvbcPspIRAx6S1lRxkq02FJJmhdBkG+4lfgjMkMuokBi44
lNIlxYa6HSIF/zYtmKITlqdV2H/nZgB59ggsuY8O0KQvgBuHXOYgATSap
mNNdUHsFKL3mvWokqDZaRNQWAwm++9ECQQDX1l4vh4Ns0n50fnF
BS4nNAwE4jdhki3QumlC6O3TG4iBZHUaBffy181EAyNMJBNcogNcmgt
6Zhbyh8bVXlW6MS8tUccSJMT1mYSuljRUjrlArpKuLAPeaETlB3u8sReb1
sd5hEjv/nxPqjQJAATEz7/tFpJl9FJOmOIAcUL+VgCR4b4W9rlw5qe2uJXM
WTqe0vf5eKPshKc6r5tFxO5BpzNmxTQ1IJNbrveVXuQJAOAcIgR0145wi1
mgcFL+nvrOFF9+brJmxmXvneqFSqtFugonfRgUMKAjj4wUxKpT616OKi
oYBDfqowlmS22LHEQJASjLp59Z8VBcR0AKcpvMCRq8Zm6Do9IqGY0V
gsKcfe9Be+OB+HfaCjdKcVJpTUwTkv6gXHLqGBEYmcO17CEwsmA==---
--END RSA PRIVATE KEY-----

Példa a Diffie – Hellman paraméterre

- -----BEGIN DH PARAMETERS-----
  MIGHAoxahLlKoH1u4FrFyNvoPUGpdctd1OrWJ
  a/ciX8DmadfSIThOwxrYIOE7oPm0AaQb+d2QB
  Er1gxWdnhzoyHfnwF/X+gQnWKkU0lsPFujlQDT
  nrWcRZ4R6Ad85tSaND3iyQc0zoBo2t3MM/GTs
  wlkTzA4i0ZD5Te3PKNKm8jAgEC
  -----END DH PARAMETERS-----

- Ez a paraméter a kulcsok létrehozásakor véletlenszerű idő alatt véletlen számokat generál

Szerver induló készlete

- Server.key – A szerver kulcsa
- Server.crt – A szerver aláírása
- Ca.crt – a hitelesítés alapja
- Dh1024.pem – Diffie- Hellmann paraméter
- Server.ovpn – A szerver oldal konfigurációs állománya

Kliens induló készlete

- Ca.crt – A kliens szerver általi hitelesítésének aláírása
- Kliens.crt – kliens aláírása
- Kliens.key – kliens kulcsa
- kliens.ovpn – konfigurációs állomány

Egy szerver beállítása

```
#Ezen az IP-n és ezen a porton akarok kapcsolódni
# Local 192.168.0.1
port 1194

;remote xy.homeip.net                # Milyen IP-ről fogad csatlakozást (nem kötelező)

#A szállítási protokoll
proto tcp
dev tun

ca ca.crt                            #szerver oldali kulcsok
cert pfsense.crt
key pfsense.key
dh dh1024.pem

server 192.168.1.0 255.255.255.0     ;Ez itt a szerver adata – ehhez fog kiosztani IP-t az OpenVPN szerver

#Ez itt a virtuális cimhez tartozó routolás
push "route 192.168.1.0 255.255.255.0 192.168.1.1”
push "dhcp-option DNS 192.168.1.1"

#Kliens beallitas
client-config-dir ccd
```

Szerver beállítás folytatása

```
comp-lzo                    ; tömörített forgalom
max-clients 20              ;kliensek maximális száma

verb 3                      ;logolás  részletessége
mute 20                     ;ismétlődések száma után mi legyen

keepalive 10 60             ; a csatorna nyitvatartása
ping-timer-rem              ; ping-gel tartja nyitva
persist-key                 ;állandó kulcskezelés, ha megszakad a kapcsolat ua. IP-vel veszi vissza.
persist-tun
```

A Petrik tűzfal konfigurációja (FreeBSD)

```
Daemon                                                  //Daemonként Fut
keepalive 10 60                                         //Timeout ideje
ping-timer-rem
persist-tun                                             //Kulcsok fajtái
persist-key
dev tun
proto tcp-server                                        //A használt protokoll TCP, de lehetne UDP is
cipher BF-CBC                                           //titkosítás módja
up /etc/rc.filter_configure
down /etc/rc.filter_configure
server 10.0.1.0 255.255.255.0                           //szerver virtuális IP címe
client-config-dir /var/etc/openvpn_csc
push "route 10.1.0.0 255.255.0.0"
lport 1194                                              //kapcsolódási port
push "dhcp-option DOMAIN petrik.local„                  //egyéb paraméterek
push "dhcp-option DNS 10.1.0.1"
push "dhcp-option WINS 10.1.0.1"
ca /var/etc/openvpn_server1.ca                          //Kulcskezelés
cert /var/etc/openvpn_server1.cert
key /var/etc/openvpn_server1.key
dh /var/etc/openvpn_server1.dh
comp-lzo
persist-remote-ip
float
push "route 10.1.0.0 255.255.0.0„                       //routolási szabályok
push "route 10.2.0.0 255.255.255.0„
push "route 195.199.255.0 255.255.255.0"
```

Windows kliens konfigurációja

```
float
port 1194                          //A kliens által használt port
dev tun
proto tcp-client                   //TCP-t használunk
remote xy.dyndns.org 1194          //Távoli szerver neve és portja
ping 10                            // A kapcsolat ne szakadjon meg
persist-tun
persist-key
tls-client
client
ca ca.crt                          //kulcsok kezelése
cert dellzoli.crt
key dellzoli.key
ns-cert-type server
comp-lzo
Pull                               //Kapja meg a szervertől a routolási
                                   // és egyéb paramétereket
verb 4                             //A Logolás szintje?
```

További információk

- http://Openvpn.net – angol
- http://www.fzolee.hu/framework/openvpn_egyszeruen – magyar
- http://wiki.hup.hu/index.php/Az_OpenVPN_finomhangol%C3%A1sa – magyar
- http://www.kfki.hu/cnc/vpn/docs/openvpn.html – magyar

Mire használható egy OpenVPN egszerű földi halandó számára?

- Tűzfalon tiltanak URL-eket – Menjünk át OpenVPN-en az othhoni gépre és onnan lépjünk tovább