Linuxos kiszolgálót mindenkinek! (9. rész)

A SuSE Linux, mint kiszolgáló, kisvállalati és otthoni környezetben.

Cikksorozatom eddigi részeiben a Kedves Olvasó megismerkedhetett sok hasznos szolgáltatással, amellyel a felhasználóinkat elkényeztettük. Most nézzünk egy újabb hasznos szolgáltatást, amellyel a felhasználókat fizikai helyüktől függetlenül hálózatba tudjuk fogni. Mostani cikkemben a virtuális magánhálózatokkal (VPN – ***Virtual Private Network***) foglalkozunk.

Egy kis elmélet

A VPN egy olyan szolgáltatás, amellyel bármilyen meglévő hálózati infrastruktúra felett saját hálózati környezetet tudunk kialakítani. Ennek segítségével megtehetjük, hogy meglévő hálózatunkat daraboljuk egymástól látszólag független hálózati egységekre, de azt is, hogy a felhasználóink a rendszerben számukra elérhető szolgáltatásokat az Interneten keresztül is biztonságos módon vehessék igénybe – mintha csak a helyükön ülnének. Ebben az esetben számukra teljesen átlátszó módon bekapcsoljuk őket a hálózatba, így a gépük olyannak fog tűnni, mintha az tényleg a lokális hálózatban lenne. A megoldás előnye, hogy sokkal biztonságosabb, mintha a tartalmakat az interneten tennénk hozzáférhetővé. Így ugyanis csak az férhet hozzá, aki a VPN elérésére jogosult, ráadásul az a megoldás kétirányú elérést tesz lehetővé. Tehát nem csak a VPN-en keresztül a hálózatba lépő felhasználó használhat erőforrásokat, hanem a hálózat tagjai is használhatják az Interneten keresztül VPN-nel csatlakozó felhasználók erőforrásait és szolgáltatásait.

És a gyakorlat

Ejtsünk pár szót a VPN működésének megvalósításáról. Amikor VPN kiszolgálót létesítünk, nem árt ha tisztában vagyunk azzal miként is valósul meg külső gépek bekapcsolása a lokális hálózatba. Mivel a VPN-be csatolt külső gépek potenciális kockázatot jelenthetnek, a tűzfalunk hangolását és a szolgáltatások elérésének korlátozását a VPN működéséhez kell igazítanunk.

A következőkben tárgyalt megoldások mindegyike úgy működik, hogy a VPN kliensek által elérhető publikus kiszolgálóra telepítjük a VPN démont, amelynek feladata, hogy a használt kiszolgálótól függően adott kapun várakozzon és figyelje a kapcsolódó klienseket.

Amint egy kliens megszólítja a szervert, az valamilyen azonosítási folyamat után becsatolja a klienst a hálózatba, mégpedig úgy, hogy mind a kliens, mind a kiszolgáló oldalán megjelenik egy virtuális hálózati csatlakozó, amelyen keresztül a kiszolgáló és a kliens bonyolítani tudja a kommunikációt. Az új csatlakozó megjelenése a rendszerben legkevesebb annyit jelent, hogy a gépek közötti elérések biztosításához módosítanunk kell a rendszerek útvonal választási tábláit (***route tables***), hiszen a VPN kiszolgáló a LAN és a VPN kliens között egy átjárót (***gateway***) fog jelenteni. Ideális esetben ezen az átjárón üzemeltetünk egy tűzfalat is, amely a VPN felől érkező klienseket az Internet felől érkező klienseknél megbízhatóbbnak kezeli, de semmiképpen nem biztosít minden olyan jogot, amit egy olyan gép kaphat, amely fizikailag a lokális hálózatban foglal helyet. Összefoglalva, a VPN kiszolgáló- és kliensoldalán egy-egy új, virtuális hálózati csatoló jelenik meg, amelyek a fizikai hálózati csatoló egy adott kapuját használva valósítják meg az adatátvitelt. Ezt az egy kapun történő kommunikációt nevezik alagutazásnak (***tunneling***). Az azonban, hogy a két VPN fél közötti adatfolyamot egy csatornába kényszerítettük még nem biztosíték arra, hogy ez a kommunikációs csatorna megbízható. Ugyan nem kötelező, de nagyon ajánlott valamilyen titkosítás használata, ugyanis ezzel nagyban megnehezíthetjük az esetleges támadó dolgát. A titkosításra ismertek szimmetrikus és nyílt kulcsú titkosítási megoldások is.

VPN megoldások

Ha úgy döntünk, hogy VPN-re van szükségünk és ezt egy Linux kiszolgáló segítségével szeretnénk megvalósítani, akkor minden bizonnyal leülünk a gép elé és elkezdünk keresgélni az Interneten. Ha ezt tesszük, akkor biztosak lehetünk abban, hogy találunk is jó néhány megoldást a problémára. Viszont ekkor felmerül a következő kérdés: Melyiket válasszuk? Nos, ez már nem ilyen egyszerű. Tulajdonképpen minden megoldásnak vannak előnyei is és hátrányai is, így – mielőtt valamelyik megvalósítás üzembe helyezése mellett döntünk – nem árt átgondolni, hogy mire is van szükségünk tulajdonképpen.

A VPN-t használhatjuk arra, hogy különböző operációs rendszerrel megáldott külső munkaállomásokat kapcsoljunk egy hálózatba, úgy, hogy azok csatlakozása a használt operációs rendszertől független legyen, és lekezelje azt a problémát, hogy a kliens helye, IP címe nagy valószínűséggel nem állandó – például egy notebook esetében. Előfordulhat ugyanakkor az is, hogy nem külső munkaállomásokat szeretnénk becsatolni, hanem több, egymástól független lokális hálózatot szeretnénk egy nagy virtuális

hálózattá összekötni, vagy éppen egy nagy lokális hálózatot szeretnénk több kis virtuális hálózatra osztani. Utóbbi esetben nagy valószínűséggel olyan kiszolgálókkal dolgozhatunk, amelyeknek az IP címe állandó és – optimális esetben – a gépek operációs rendszere is azonos: esetünkben ilyen például valamelyik Linux változat.

Noha első ránézésre nincs nagy különbség a két említett probléma között, azt azért jó tudni, hogy a két összeállításra más-más megoldás az optimális.

Nézzük meg a kínálatot, milyen megoldások állnak rendelkezésünkre. Használhatjuk VPN kialakításához a Poptop csomagot, az OpenVPN csomagot, vagy a Freeswan IPSec implementációját. Természetesen találhatunk egyéb megoldásokat is, ezek az általam használt és bemutatni kívánt rendszerek.

A Poptop egy Linuxos PPTP kiszolgáló. A PPTP (Point to Point Tunneling Protocol) egy Microsoft fejlesztésű VPN megoldás, amellyel meglehetősen egyszerűen csatolhatunk Windowsos és Linuxos PPTP klienseket a virtuális magánhálózatunkba. Amennyiben könnyen, gyorsan konfigurálható és egyszerűen használható VPN megoldást keresünk, akkor ez nagyon jó megoldás lehet. Különösen jól használható olyan környezetben, ahol a VPN kliensek valamilyen Windows operációs rendszert futtató gépek.

A Poptop rendszer egy PPTP protokollt társít a Linux PPP kiszolgálójához, így a rendszer a telefonos betárcsázáshoz teljesen hasonló módon konfigurálandó.

A Poptop szerverről bővebben a ➲ http:\\www.poptop.org címen olvashat az érdeklődő.

Az OpenVPN egy könnyen használható, SSL támogatást biztosító VPN démon, amelyhez létezik Linux és Windows oldali szoftver is, így ez is használható heterogén rendszerekben. Posix rendszereken való használatnál az OpenVPN csomag telepítése után létre kell hoznunk a megfelelő virtuális hálózati csatlakozókat, amelyeken keresztül a kommunikáció folyik majd. Ezután a VPN csatorna két oldalán el kell indítani egy parancssoros démont, amelyet a megfelelő paraméterekkel ellátva felépül a hálózatokat összekötő csatorna. Windowsos kliens esetében a projekt weboldaláról letölthető telepítőt kell lefuttatni, amely utána a rendszerben virtuális csatlakozókat fog létrehozni, amely csatlakozókon keresztül tudjuk a VPN erőforrásait elérni.

Az OpenVPN tartalmaz SSL támogatást, ami annyit jelent, hogy a kommunikációs csatorna forgalmát mindkét oldalon nyílt kulcsú titkosítási módszerrel titkosítjuk, így a csatorna forgalmának lehallgatása gyakorlatilag lehetetlenné válik. A módszer hátránya, hogy a kódolás erős gépet, vagy cél-eszközt igényel. Az OpenVPN projekt megtalálható az ➲ http:\\www.openvpn.sourceforge.net weboldalon.

Az IPSec (***Internet Protocol SECurity***) egy erős biztonsági megoldásokkal ellátott protokoll, amelyet az IETF (***Internet Engineering Task Force***) fejlesztett ki és amely megoldás az IPv6-nak már alapszolgáltatása lesz. IPv4-es rendszerünket is felkészíthetjük az IPSec támogatására, ha a megfelelő rendszermag módosításokat elvégezzük, valamint telepítjük a felhasználói csomagokat.

A fentiekből is látszik, hogy az IPSec több mint egy VPN megoldás: ez egy alacsony szinten megvalósított biztonsági megoldás. Az IPSec protokollnak több implementációja létezik, ebből az egyik az általam említett Freeswan/IPSec.

Emellett léteznek egyéb fejlesztések is, így például a Windows operációs rendszerek egy a Microsoft által készített IPSec megoldást tartalmaznak. Mivel az IPSec hamarosan, az IPv6 bevezetésével és széles körű elterjedésével a mindennapok részévé fog válni, ezért érdemes megismerkedni vele, érdemes tudni miként működik.

A Freeswan/IPSec projektről az érdeklődők egy kiterjed és nagyon alapos dokumentációt találnak a ➲ http:\\www.freeswan.org címen.

Használat a gyakorlatban

Gyakorlati útmutatónk alkalmával a Poptop és az OpenVPN projektek kínálta megoldásokat tanulmányozzuk át részletesen. A Suse 9.0-s verziója már tartalmazza mindegyik szolgáltatást, ellentétben a 8.2 kiadással, amely csak az OpenVPN csomagot tartalmazza. Ettől még nem kell megijedni, a projektek weboldaláról minden esetben letölthetőek a legfrissebb telepítő készletek, így azok akármelyik Linux kiadáshoz telepíthetőek.

Suse 9.0 esetén a telepítés meglehetősen egyszerű. A YaST csomagtelepítőjében a megszokott módon megkeressük a kívánt csomagokat és telepítjük. Innentől kezdve a telepített rendszer konfigurálható, használható.

Poptop kiszolgáló beállítása

Először nézzük a Poptop PPTP kiszolgáló beállítását. Ehhez telepíteni kell a Poptop csomagot, valamint a PPP csomagot, és a rendszermaghoz PPP támogatást kell biztosítani. Amennyiben a PPP modul le van fordítva, úgy az */etc/**modules.conf*** állományban be kell jegyezni, amennyiben nincs a rendszermaghoz PPP támogatás, úgy a támogatás bekapcsolásával újat kell fordítanunk. (A Suse által telepített rendszermaghoz van PPP modul fordítva, így annak fordításával nem kell bajlódnunk. Amennyiben ADSL, vagy modemes kapcsolatot használunk, úgy a PPP meghajtó minden bizonnyal be van töltve, ugyanis az szükséges az előbb említett kapcsolatok kezeléséhez.)

Miután telepítettük a PPTP kiszolgálót néhány konfigurációs állományban módosításokat kell elvégeznünk. Ezen módosításokat most a dokumentáció alapján nézzük.

Amennyiben valamelyik állomány a mi rendszerünkben más helyen található, úgy ott az elérési utakat értelemszerűen módosítani kell. Az első módosítandó állomány a már említett */etc/**modules.conf***. Itt a következő modulok betöltését kell bejegyezni:

```
alias char-major-108 ppp_generic
alias tty-ldisc-3 ppp_async
alias tty-ldisc-14 ppp_synctty
alias ppp-compress-18 ppp_mppe
alias ppp-compress-21 bsd_comp
alias ppp-compress-24 ppp_deflate
alias ppp-compress-26 ppp_deflate
alias net-pf-47 ip_gre
```

A PPTP démon alapbeállításait az */etc/**pptpd.conf*** állományban találjuk meg. Ez az állomány nem tartalmaz túl sok beállítást, mindössze azt mondja meg, hogy a PPP beállítási állomány pontosan hol található, valamint egy IP-t ad a kiszolgáló VPN interfészének és egy IP tartományt ad a csatlakozó klienseknek.

Egy példa az */etc/pptpd.conf* állományra:

```
option /etc/ppp/options.pptpd
#debug
localip 192.168.0.1
remoteip 192.168.0.200-249
```

A fenti konfiguráció azt mondja, hogy a PPTP démon PPP állománya az */etc/ppp* könyvtárban az *options.pptpd* állományban van, a kiszolgáló a 192.168.0.1-es címet kapja és a kliensek a 192.168.0.200 és a fölötte lévő 50 címből gazdálkodhatnak. A debug kapcsoló bekapcsolásával elérhetjük, hogy a démon teleírja a naplót a futási állapot üzeneteivel, így adva egy nagyszerű eszközt az esetleges hibák elhárításához. A *pptpd.conf* állományban megnevezett PPP konfigurációs állományt az alábbi tartalommal lássuk el:

```
lock
#debug
name pptpd
nobsdcomp
proxyarp
ms-wins <hálózati-wins-kiszolgáló-ip-címe>
ms-dns <hálózati-dns-kiszolgáló-ip-címe>
```

Ezzel a beállítással egy titkosítás nélküli VPN csatornát létesítünk, ami ugyan működő megoldás, de nem egy biztonságos összeállítás. A Poptop PPTP kiszolgáló ellátható SSL titkosítással is, amennyiben a kiszolgálóhoz tartozó MPPE foltot is telepítjük. A foltozás letölthető a Poptop projekt weboldaláról is. Amennyiben telepítettük az MPPE és ChapMS kiegészítést, úgy az alábbi sorokat hozzáadva az *options.pptpd* állományhoz elérhetővé tehetjük a Windows kliensek által is titkosítást:

```
-chap
-chapms
+chapms-v2
mppe-40
mppe-128
mppe-stateless
```

A fenti szolgáltatások elérhetőségét, szükségességét az alábbi sorok értelemszerű beszúrásával állíthatjuk:

```
#refuse-pap
#refuse-chap
#refuse-mschap
#require-mschap-v2
#require-mppe
```

Ha végeztünk az *options.pptpd* állománnyal, akkor az */etc/ppp/chap-secrets* állományban megadhatjuk, hogy melyik felhasználó milyen jelszóval milyen gépről érje el a szolgáltatást. Ehhez mindössze egy sort kell felhasználónként beszúrni, ami a következőképpen néz ki:

```
felhasználó_neve pptpd "jelszó" <IP tartomány>
```

Pédául:

```
viktor pptpd "passwd" 192.168.0.100
```

Ezzel a viktor nevű felhasználó a passwd jelszóval a 192.168.0.100-as című gépről tud bejelentkezni. Amennyiben az IP cím helyére *-ot teszünk, akkor az az IP korlátozás teljes feloldását jelenti. Ha ezzel végeztünk, akkor nincs is más dolgunk, mint újraindítani a pptp kiszolgálót és már csatlakozhatunk is a géphez. Amennyiben a PPTP kiszolgáló tűzfallal védett, ne felejtsük el engedélyezni a 1723-as TPC és UDP portot. A Poptop kiszolgáló teljes dokumentációja és további érdekes és hasznos információk megtalálhatóak a projekt honlapján.

Az OpenVPN projekt

Az OpenVPN kiszolgáló telepítéséhez a YaST csomagtelepítőjével az *openvpn* csomagot kell telepítenünk. Ezután az */usr/sbin* könyvtárban megjelenik az *openvpn* nevű futtatható állomány. OpenVPN esetén alapesetben ezen az állományon kívül nem is lesz szükségünk semmilyen más konfiguráció elkészítésére, parancssorból paraméterezve tudjuk futtatni a kiszolgálót. Ez előtt azonban kell még tennünk egy-két előkészületi lépést. Amennyiben 2.4.7-esnél frissebb rendszermagot használunk – ami egyébként elég valószínű –, akkor telepítenünk kell a TUN/TAP meghajtót. Ha ez megvan, akkor létre kell hoznunk a */dev/net/tun* nevű eszközt az alábbi paranccsal `mknod /dev/net/tun c 10 200`, majd töltsük be a meghajtót a `modprobe tun` parancs futtatásával. Ha rpm csomagból telepítjük a programot, akkor az eszköz létrehozására nincs szükség, mert ezt a telepítő elvégzi. Amennyiben a kiszolgálón tűzfal fut, úgy ne feledkezzünk meg a tűzfalon a tun eszköz megfelelő beállításáról sem! Ha a fentiekkel mind elkészültünk, akkor jöhet amire vártunk, indíthatjuk a kapcsolatot. Ez, mint már említettük, parancssorból történik. Íme egy séma egy egyszerű, titkosítás nélküli VPN csatorna létrehozására:

```
openvpn --remote <ellenoldali-gép-hostneve> --dev
➥tun1 --ifconfig <helyi-tun-csatoló-IP-címe>
➥<távoli-tun-csatoló-IP-címe>
```

Nézzünk egy példát. Van két helyi hálózatunk, ahol az egyik hálózat átjárójának címe gw1.hu, míg a másik hálózat átjárójának címe gw2.hu, valamint a gw1.hu gépen 10.1.1.100 címet adunk a tun1 hálózati csatolónak, míg gw2.hu gépen 10.1.1.200-at. Ezután a gw1 gépen az alábbi parancsot kell futtatni:

```
openvpn --remote gw2.hu --dev tun1 --ifconfig
➥10.1.1.100 10.1.1.200
```

A másik, tehát gw2.hu gépen pedig a következő paranccsal építhető ki a kapcsolat:

```
openvpn --remote gw1.hu --dev tun1 --ifconfig
➥10.1.1.200 10.1.1.100
```

Mint látható a kapcsolat felépítése rendkívül egyszerű. Természetesen lehetőségünk van arra, hogy titkosított csatornát használjunk a kommunikáció során. Az OpenVPN támogat mind szimmetrikus, mind TLS alapú titkosítási módszereket, így mindenki választhat igényének megfelelően. Azok, akinek az érdeklődét sikerült felkelteni a VPN iránt, bőséges olvasnivalót találnak a témában a projektek honlapjain. Ezzel a cikkel a Suse Linux-ról szóló cikksorozatom végére értünk. Remélem sikerült kedvet csinálnom, nemcsak a Suse, de akármelyik Linux kiadás megismeréséhez.

Illés Viktor