Bevezetés a FreeS/WAN használatába (1. rész)

VPN-alagutak biztonságos vezeték nélküli és más világhálós kapcsolatok kiépítésére.

A legutóbbi, mintegy ötéves időszak során az IPSec a VPN-kapcsolatok vezető szabványává fejlődött. A FreeS/WAN (➲ http://www.freeswan.org) nyílt forrású, kiterjedt biztonságos számítógép-hálózat, a legnépszerűbb és az egyik legérettebb IPSec-megvalósítás, ami Linux-rendszereken működik. A mostani alkalommal és a következő hónapban azt fogjuk megvizsgálni, miért és hogyan kell a FreeS/WAN-t biztonságos hálózati adatcserére használni. Eme vizsgálódásunkat a vezeték nélküli (rádiós) hálózatokkal kezdjük.

VPN-alapok

Mindeddig a VPN-ek két leggyakoribb használati formája a két hálózat közötti kapcsolat volt. A telephelyek közti kapcsolatoknál mindegyik telephely, illetve hálózat saját VPN-átjáróval rendelkezik, azaz olyan VPN-kiszolgálógéppel, amely az IPSec-en vagy más VPN-protokoll alapú alagutakon keresztül tart fenn kapcsolatot más VPN-átjárókkal, ahogyan az az *1. ábrán* látható.

Ez a kiszolgálógép ugyanakkor a helyi hálózatra csatlakozó gépek számára útválasztóként is működik, hogy az egyes csomagokat más kapcsolódó VPN-helyekhez eljuttassa. Mindez más szóval azt jelenti, hogy egy telephelyek közti VPN-hálózatban több felhasználó, illetve számítógép osztozik egyetlen alagúton, hogy adatokat cseréljenek a távoli hálózatra csatlakozó számítógépekkel.

A távoli hozzáférésű VPN-ek, ideértve a vezeték nélküli hálózatokban használatos fajtát, ettől kicsit eltérőek. A VPN-alagút ahelyett, hogy egy teljes számítógépes hálózatot egy másikhoz kapcsolna, mindössze egyetlen felhasználó vagy számítógép és egy távoli hálózat között teremt kapcsolatot (*2. ábra*). A felhasználó helyi VPN-átjárója jellemzően alkalmazói program, amely a helyi gépen fut. A távoli VPN-átjáró rendszerint tűzfal vagy egy kijelölt VPN-készülék a gazdahálózaton.

A vezeték nélküli helyi hálózatból (LAN) épített VPN-ek a távoli hozzáférésű VPN-ek fontos alcsoportját alkotják. A vezeték nélküli hálózatok az általuk biztosított kényelemnek és az alacsony költségeknek köszönhetően egyre népszerűbbek. Minthogy azonban a nevüknek megfelelően az adatok közvetítéséhez rádióhullámokat használnak, könnyű őket lehallgatni.

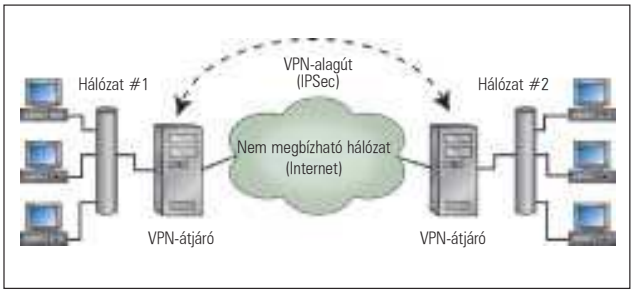
A hálózati termékek gyártói a vezetékes hálózatnak megfelelő titkosítás biztosítására tettek erőtlen kísérletet a vezeték nélküli titkosítási szabvány (Wireless Encryption Standard – WEP) megalkotásával, de a WEP-et a titkosítás megvalósításának hibái szinte azonnal elavulttá tették. Emiatt sok vezeték nélküli hálózatot használó vállalat máris elfordult a WEP-től. Helyette inkább VPN-alagutakat használnak a vezeték nélküli kapcsolatok titkosítására.

A 2. ábrához visszatérve meg kell említenünk, hogy egyetlen rendszer képes összetett VPN/vezeték nélküli átjáróként dolgozni. A *3. ábrán* újabb lehetséges hálózati elrendezést láthatunk: mind a vezeték nélküli egység, mind a VPN-átjáró önálló egységet alkot.

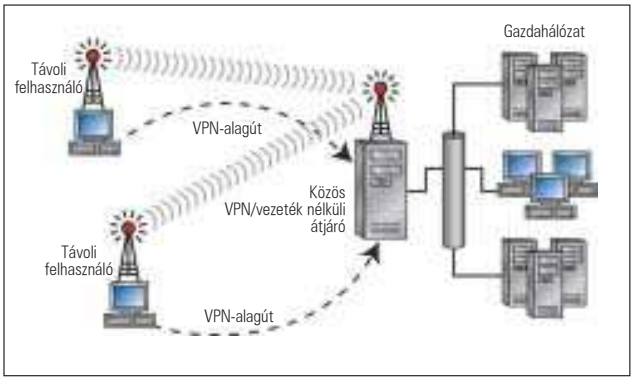
Az IPSec és a FreeS/WAN

Mint azt már korábban kijelentettem: az IPSec a legnépszerűbb VPN-protokoll. Minthogy ez az IP-protokoll kiterjesztése, ez az Internet „hivatalos” VPN-protokollja. Szinte az IPSec létezése óta ***John Gilmore*** és a FreeS/WAN kezdeményezés fejlesztőcsapata a FreeS/WAN csomag kifejlesztésével és a Linux számára történő átadásával minden tőle telhetőt megtett az IPSec minél szélesebb körű elfogadásáért.

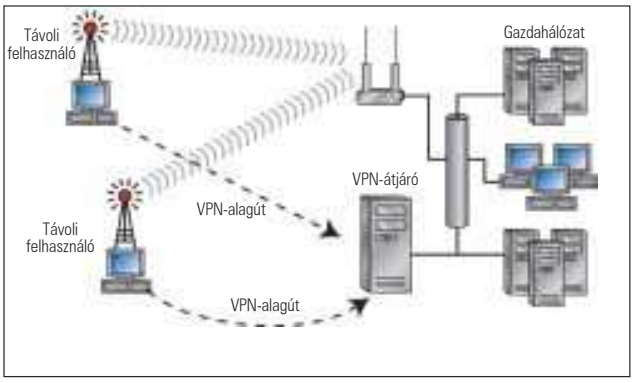
A FreeS/WAN legfrissebb változatáról szóló végleges adatok a kezdeményezés honlapjáról,



1. ábra A telephelyek közötti VPN-kapcsolat



2. ábra A vezeték nélküli – távoli hozzáférésű – VPN



3. ábra Egy másfajta LAN VPN-elrendezés

a ➲ http://www.freeswan.org címről szerezhetők be.
Egy szó, mint száz, a FreeS/WAN érett, jól dokumentált és támogatott program. Ha Linuxot használsz, akkor VPN-szükségleteid kielégítésére a FreeS/WAN a megfelelő választás.

A FreeS/WAN beszerzése és telepítése

A NetFilterhez hasonlóan a FreeS/WAN is a tényleges munkát végző rendszermagmodulból és a felhasználói felületekből áll, az utóbbiak a beállítást szolgálják. A NetFiltertől eltérően azonban a FreeS/WAN nem szerepel a Linux-rendszermag forráskódcsomagjai között, így a legtöbb változathoz adott rendszermagban nem is bukkan fel. Ez számos ország titkosítási eljárások korlátozása miatt van így.
A rendszermag újraépítése, esetleg újrafordítása a FreeS/WAN telepítése esetlen módjának tűnik. Ennek elkerülése érdekében számos Linux-változat, többek között a SuSE, a Debian és a Mandrake olyan FreeS/WAN-változatot tartalmaznak, amelyik képes az adott változathoz tartozó rendszermaggal együttműködni.
A Red Hat 7.3 Linux-változat felhasználói számára IPSec-képes rendszermagcsomagok – mind bináris, mind forráskód formában –, valamint a FreeS/WAN telepítőeszközei a Steamballoon telephelyéről, a ➲ http://rpms.steamballoon.com/freeswan címről tölthetők le.
Mivel jómagam leginkább SuSE és Red Hat Linux-változatokat használok, a FreeS/WAN program ezekhez a rendszerekhez történő beszerzését és telepítését fogom az alábbiakban ismertetni. Abban az esetben, ha az igényeid összetettebbek, leírás végett látogass el a ➲ http://www.freeswan.org/doc.html címre. Linux-változatodtól és a rendszermag frissességétől függően lehetséges, hogy a rendszermagot újra kell fordítanod, de ennek a folyamatnak a pontos leírása megtalálható a webhelyen.

A FreeS/WAN telepítése SuSE rendszerekre

Abban az esetben, ha a Linux-változathoz járó eredeti rendszermagot használod, egyszerűen telepítsd a sec-sorozatban szerepelő `freeswan.rpm` csomagot. Győződj meg róla, hogy az `ipsec.o` modul rendszermagváltozata megfelel az üzemelő SuSE rendszer rendszermagváltozatának.
Egy csapásra mindkét ellenőrzést elvégezhetjük: a futó rendszer magjának változatszámát a `uname -av` parancs kiadásával kérdezhetjük le. Az egyelőre telepítetlen `freeswan.rpm` csomag rendszermagváltozatát az alábbi paranccsal tudhatjuk meg:

```
# rpm -ql -p ./freeswan.rpm | grep -e ipsec.o
```

A rendszermag változatszámát az erre az állományra mutató útvonal fogja megmutatni, tehát a példának megfelelően */usr/lib/modules/2.2.18/ipv4/ipsec.o*. Ha a változatok azonosak, akkor telepítsd a csomagot:

```
# rpm -Uvh ./freeswan.rpm
```

Ezután a */etc/rc.config* állomány megnyitásával és a START_IPSEC változó értékének „yes”-re állításával kapcsold be az IPSec-et. Most érkezett el az ideje, hogy helyettesítsük a géphez tartozó titkosítási kulcsot – az RSA-aláírás kulcspárt –, amelyet a FreeS/WAN.RPM-ek telepítettek a rendszeredre.
Ha a */etc/ipsec.secrets* állomány létrehozási dátuma az aznapi (mai) dátumnál korábbi, akkor bizony új kulcsokra van szükség. Ennek megtételéhez a FreeS/WAN 1.92-es vagy annál magasabb változatszámmal ellátott változatoknál az alábbi parancsokat használhatjuk:

```
# mv /etc/ipsec.secrets /etc/ipsec.secrets.test
# ipsec newhostkey --hostname my.host.FQDN
➥--output /etc/ipsec.secrets --bits 2192
```

Természetesen a `my.host.FQDN` kapcsoló helyett a géped teljes nevét kell begépelned, például: `george.wiremonkeys.org`. A FreeS/WAN korábbi változatainál a következő parancsot használhatjuk:

```
# ipsec rsasigkey --hostname my.host.FQDN
➥2192  > /etc/ipsec.newkey
```

Ha használtad az `ipsec rsasigkey` parancsot, akkor szövegszerkesztővel meg kell nyitnod a */etc/ipsec.secrets* állományt, és az ott kapcsos zárójelek ({ }) között szereplő jelsorozatot ki kell cserélned az `ipsec.newkey`, vagy bármilyen más állományba irányított új kulccsal. Annak ellenére, hogy még be sem állítottad a szolgáltatást, máris elindíthatod és ellenőrizheted:

```
# /etc/init.d/ipsec start
# ipsec whack --status
```

Ha a második parancs (az `ipsec whack --status`) `000` visszatérési kóddal ér véget, FreeS/WAN-telepítésed megfelelően működik.

FreeS/WAN telepítése Red Hat-változatokra

Ha a Red Hat 7.3-as változatot a rendszerhez adott eredeti rendszermaggal üzemelteted – ez a cikk írásának idején a 2.4.18-as volt –, akkor először is szerezd be az IPSec-képes rendszermagcsomagot a
➲ http://rpms.steamballoon.com/freeswan címről, vagy a 44-es CD Magazin/FreeSWAN könytárból. Innen akár a forrást, akár a futtatóbinárist letöltheted; először a rendszermagcsomagot telepítsd.
Ha Linux-rendszeredben a rendszerhez adott eredeti rendszermagcsomag van telepítve – majdnem biztos, hogy az –, akkor használnod kell a `--force` kapcsolót, mivel a Steamballoon FreeS/WAN rendszermagcsomagjának bázisneve („kernel”) megegyezik a Red Hat-változat rendszermagjának csomagnevével. Celeron alapú Red Hat 7.3-as rendszeremen a Steamballoon rendszermagcsomagot így telepítettem (a példákban szereplő valamennyi változatszám mára már bizonyára elavulttá vált):

```
# rpm --force -i ./kernel2.4.18-3ipsec.i686.rpm
```

Felesleges aggódnod a `--force` kapcsoló kényszerítő jellege miatt, mivel a rendszermag lenyomatállományának nevei és a modulkönyvtárak mind egyediek, és régi rendszermagodat nem fogják felülírni. A saját Red Hat 7.3-as rendszeremet alapul véve az új rendszermag lenyomatállomány például a */boot/vmlinuz-2.4.18-3ipsec*, a modulkönyvtár pedig a */lib/modules/2.4.18-3ipsec* címen lesz elérhető. A Steamballoon RPM csomagjában levő telepítés utáni héjprogram felülírta a rendszermagra mutató bejegyzést a */boot/grub/grub.conf* fájlokba az új IPSec-rendszermagra mutató új bejegyzéssel – tulajdonképpen a betöltőmenüből eltávolította a régi rendszermagot. Ám amint a régi rendszermagra mutató bejegyzést ismét hozzáadtam a menühöz, rendszerbetöltéskor gond nélkül tudtam választani közülük.
A rendszermagcsomag telepítését követően telepítsd a felhasználói módú eszközöket. Az én rendszeremen ez az alábbi

paranccsal történt meg:

```
# rpm -i freeswan-1.97-0.i386.rpm
```

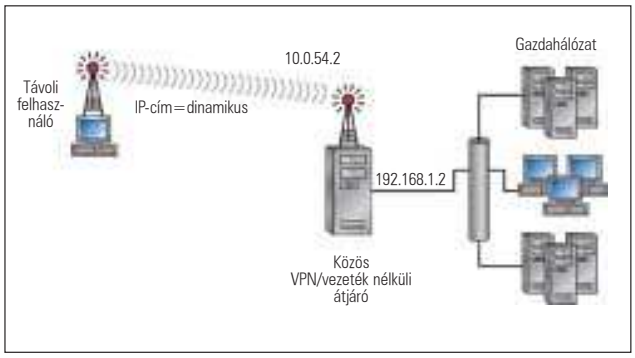
Az RPM csomag egy héjprogramot – */etc/init.d/ipsec* – telepít, de a szolgáltatást nem indítja el. Az üzembe helyezést az alábbi paranccsal végezhetjük el:

```
# chkconfig --add ipsec
```

Ezután hozz létre új RSA-kulcspárt, úgy, ahogy azt az előző szakaszban megadtam. Ha kész, máris elindíthatod és kipróbálhatod a FreeS/WAN telepítésedet szolgáltatást a már ismertetett módon.

Vezeték nélküli LAN VPN beállítása

Sajnos helyszűke miatt csak egyetlen gyakori alagutazás forgatókönyvét tudom megvizsgálni – ezt mutatja be a 2. ábra. A *4. ábra* a 2. ábrán látható hálózat egy részletét tárja fel, ezúttal



4. ábra IP-címekkel rendelkező vezeték nélküli VPN

IP-címekkel ellátva. Mint azt rövidesen látni fogjuk, nincs szükség az összes lehetséges ügyfél IP-címének ismeretére. A cikk hátralevő része több fontos alapfeltevésen nyugszik:

1. Az alapvető hálózati kapcsolatok működnek, a vezeték nélküli ügyfelek képesek kapcsolódni a kiszolgálóhoz.
2. Az alapvető csomagtovábbítás működik: a vezeték nélküli ügyfelek képesek elérni az átjáró túloldalán lévő gépeket.
3. Az átjáró egyelőre még nem működik tűzfalként.

A harmadik feltevés csupán könnyítés. A biztonság rétegekben valósítható meg, és a telepítési időn kívül semmibe sem kerül, hogy megszabjuk, a bejövő VPN-forgalom merre mehet és merre nem. Sajnos itt nem bocsátkozhatom mélyebb részletekbe; ehelyett olvasd el a ***FreeS/WAN quick start on firewalling*** HOGYAN-t a ➲ http://www.freeswan.org/doc.html címen.

Az ipsec.conf elkészítése

A FreeS/WAN beállítása két állományon keresztül történik: a */etc/ipsec.conf* a főbb beállításokat tartalmazó állomány, míg a */etc/ipsec.secrets* a kulcstár. Mindkét állománynak korlátozott engedélyekkel kell rendelkeznie; a 0600 megbízható választás. A */etc/ipsec.secrets* állományt különös gonddal kell védelmezni. Amennyiben ebből az állományból bármit ki kell másolni, mondjuk a gép nyilvános RSA-kulcsát, a szükséges adatot másold ki egy önálló állományba. Soha ne engedd meg, hogy az ***ipsec.secrets*** állomány kikerüljön a rendszeredből. Ezt az állományt

1. lista /etc/ipsec.conf a vezeték nélküli ügyfélen

```
# alapbeÆll tÆs
config setup
     interfaces=%defaultroute
     klipsdebug=none
     plutodebug=none
     plutoload=%search
     plutostart=%search
     uniqueids=yes

conn %default
     keyingtries=0
     authby=secret

conn george-gracie
     authby=rsasig
     left=10.0.54.2
     leftid=@george.wiremonkeys.org
     leftsubnet=0.0.0.0/0
     leftrsasigkey=0sAQPF0JJvY7...
     right=%defaultroute
     rightid=@gracie.wiremonkeys.org
     rightrsasigkey=0sNU0q2Y0Y0jxAIKuutV3...
     auto=start
```

részletesebben a következő hónapban fogjuk megvizsgálni. Az *1. lista* egy vezeték nélküli VPN-ügyfél ***ipsec.conf*** állományát mutatja be. A */etc/ipsec.conf* állomány három részre tagolódik: az alapvető telepítési kapcsolókra (`config setup`), az előre beállított alagútértékekre (`conn %default`), és végül az alagút-meghatározásokra (`conn george-gracie` az 1. listában, ezt a nevet magam választottam ennek az alagútnak). A `config setup` szakaszban található előre beállított jellemzők az egykártyás rendszereken biztonsággal érintetlenül hagyhatók. A legfontosabb beállítás az `interfaces`, ami megadja, hogy melyik hálózati csatoló lesz az IPSec-csatornák helyi végpontja. Az előre beállított érték, a `%defaultroute` ennek az `ipsec=[csatol ]` a feloldása, ahol a `[csatol ]` a gép alapértelmezett hálózati csatolója, általában az `eth`. Ezennel máris az ***ipsec.conf*** lényegéhez érkeztünk el: az alagút-meghatározáshoz. Az 1. listában a george-gracie alagút-meghatározásban az első sorban találjuk az `authby` beállítást, ami azt szabja meg, hogyan végezzék az egyes IPSec-gépek a saját hitelesítésüket egymás számára. Az alapérték a „secret”, amely az előzetesen megosztott titkos azonosítót jelenti. Ez a beállítás lehetővé teszi, hogy az előre meghatározott titkos karaktersorozat legyen az azonosítási kulcs. Ez elsőre meggondolatlanságnak tűnhet, de mégis biztonságos, ugyanis az azonosító sosem utazik a hálózaton.
Most más a helyzet, hiszen az 1. listában az `authby` kapcsoló `rsasig`-re van beállítva. Az RSA-hitelesítés nem szükségszerűen sokkal biztonságosabb, ezzel szemben sokkal kényelmesebb. Míg a megosztott azonosítót valamilyen biztonságos eszköz, mint például titkosított levél vagy az SSH segítségével előzetesen ki kell cserélni, az RSA-hitelesítésben használt nyilvános kulcsok akár ország-világ színe előtt kicserélhetők, mi több, még a honlapon is közzétehetők.
A FreeS/WAN beállításánál fontos a bal és a jobb oldal megkülönböztetése: ezek a parancsokban és kapcsolókban az IP-alagutak végpontjainak megjelölésére szolgálnak. Hogy melyik

2. Lista /etc/ipsec.conf az átjárón

```
config setup
     interfaces="ipsec0=eth1"
     # Ös  gy tovÆbb
     forwardcontrol=yes

conn george-gracie
     authby=rsasig
     left=10.0.54.2
     leftid=@george.wiremonkeys.org
     leftsubnet=0.0.0.0/0
     leftrsasigkey=0s0sAQPF0JJvY7xK9Cmx1...
     right=%any
     rightid=@gracie.wiremonkeys.org
     rightrsasigkey=0sNU0q2Y0Y0jxAIKuutV3...
     auto=add
```

elnevezés melyik oldalt jelöli, tulajdonképpen lényegtelen, az a fontos, hogy a jelöléseket következetesen alkalmazzuk. Ugyanannak a gépnek mindkét alagút-meghatározásban jobb oldalinak kell lennie, és egy rendszernek sem szabad megfordítania a másik gépen szereplő bal–jobb kiosztást.

A biztonság kedvéért, amikor egy gép egy másik számítógép számára kiszolgálóként működik, ezt a gépet javasolt bal oldaliként feltüntetni. Példánknál maradva a ***George*** nevű gép kiszolgálóként működik a vezeték nélküli ügyfelek számára, így ***George*** bal oldali, míg ***Gracie***, az ügyfélrendszer, jobb oldali.

A „bal" alagútbeállítási értéke jelzi az alagút bal oldali végpontjának IP-címét, ***George***-ot: 10.0.54.2. A jobb oldal természetesen a jobb oldali végpont IP-címét jelöli ki. Forgatókönyvünkben viszont az áll, hogy ***Gracie*** és a többi vezeték nélküli ügyfél dinamikus IP-címet kap. Ekkor egy rögzített IP-cím megadása helyett a `%defaultroute` értéket fogjuk használni, amely a gép alapértelmezett útvonalát jelöli; ez a hálózati kártyához tartozó IP-címmé fog alakulni.

Az alagút `leftid` kapcsolója felesleges ismétlődésnek tűnhet, minthogy a `left`-tel már azonosítottuk a bal oldali IP-címet, ám ez valójában egy kicsit eltér attól. A `leftid` és `rightid` kapcsoló minden alagút végponthitelesítési azonosítóját határozza meg. Ez lehet egy IP-cím, de lehet a kukac (@) jelet követő teljes név (FQDN). Minthogy a ***Gracie*** ügyfél, a dinamikus IP-cím kiosztáson keresztül kap címet, így a `leftid` számára a @gracie.wiremonkeys.org az egyetlen használható érték. Ebben a példában ugyanakkor a `rightid` számára a @george.wiremonkeys.org és a 10.0.54.2 IP-cím kölcsönösen felcserélhető értékek.

Az 1. listában a következő megfontolásra érdemes alagútbeállítás a `leftsubnet`. Ez meghatározza, hogy milyen cél-IP-címek fogadhatnak csomagokat a jobb oldaltól, emiatt azt is, hogy a jobb oldali végpontok milyen célokhoz használhatják az alagutat. ***Gracie*** és a többi vezeték nélküli ügyfél ***George***-ot használja egyedüli átjáróként a vállalati helyi hálózathoz és általában a nagyvilággal való kapcsolattartásra, ezért ezt 0.0.0.0/0-ra állítottuk, ami így az összes címet kifejezi.

Létezik egy `rightsubnet` kapcsoló is, ezt azonban kizárólag a telephelyek közti kapcsolatokban szükséges beállítani. Távoli hozzáférés vagy egyéb kiszolgálóalapú megoldásokban a két kapcsoló közül csak az egyik beállítása szükséges.

Ha az alagút számára RSA-hitelesítést írtunk elő, akkor mind a `leftrsasigkey`, mind a `rightrsasigkey` megadása kötelező. Ezek az értékek az ***ipsec.secrets*** állományban, a `#pubkey=` kezdetű sorokban találhatók meg. Az alábbi két, vagylagos jelleggel használható parancs közül választhatunk:

```
# ipsec showhostkey --left
```

vagy

```
# ipsec showhostkey --right
```

A `--left` és `--right` kapcsolók (amelyek a FreeS/WAN 1.9-es vagy annál későbbi változatában használhatók) révén a kimenet a `leftrsasigkey` vagy `rsasigkey` utasítás formátumának megfelelő alakú lesz, ami aztán az ***ipsec.conf*** állományba rugalmasan bemásolható lesz. Például a ***George*** gépen futtatott `ipsec showhostkey --left` az 1. listában bemutatott `leftrsasigkey` értéket, a ***Gracie*** gépen futtatott `ipsec showhostkey --right` pedig a `rightrsasigkey` értéket adta eredményül. Fontos megemlíteni, hogy bár az RSA-kulcsok hosszúak, mindegyiküknek el kell férnie egyetlen sorban, vagyis sortörés nem használható!

Az utolsó kapcsoló az 1. listában az alagútbeállításánál az `auto`, ami – amint az IPSec elindul – meghatározza a FreeS/WAN számára, hogy van-e tennivaló az alagút körül. A `start` érték írja elő, hogy a kezdeti értékadás és az önműködő indítás megtörténjen. Az `add` érték előírja, hogy a `pluto` nevű IPSec-démonhoz legyen hozzáadva. Az `ignore` hatására pedig figyelmen kívül hagyja az alagutat. Az 1. listában az `auto` értéke `start`-ra lett beállítva, ezért amikor csak az IPSec a ***Gracie*** gépen elindul, szeretnénk felélesztení az alagutat a ***George***-on. Az `auto` számára a `plutoload` és `plutostart` telepítésbeállítási kapcsolókat megfelelően kell beállítani azaz, hogy valamiféle értelmük legyen: részletesebb útmutatáshoz az ***ipsec.conf(5)*** súgóoldalról juthatunk.

Rendben, ez minden, amit az ***ipsec.conf*** ügyféloldali beállításáért tenni kell. De vajon mi a helyzet a kiszolgálóval? Úgy fest a dolog, hogy ebben a forgatókönyvben a beállítás mindkét oldalon közel azonos. A 2. lista mutatja a ***George*** nevű gép */etc/ipsec.conf* állományát.

Az első eltérés a ***Gracie***-géptől az, hogy ***George*** több hálózati kártyával rendelkezik, következésképpen a hálózati csatolót egyértelműen meg kell határozni. A kiszolgáló alapértelmezett útvonala a helyi hálózatra csatlakozik, és nem a vezeték nélküli hálózatra, ennek következtében a `%defaultroute` értéket nem használhatjuk.

Ezen kívül egy új telepítési kapcsolóval is rendelkezünk, a `forwardcontrol`-lal. Ha ennek értékét „yes”-re állítjuk, elő fogja írni az IPSec-nek, hogy szükség szerint kapcsolja be az IP-továbbítást, és kapcsolja ki, amint az IPSec lezárásra kerül. Továbbá magában az alagútszakaszban a `right` (jobb oldal) kapcsolót `%any`-re kell állítani, nem peidg `%defaultroute`-ra, hiszen a `%defaultroute` *George* helyi hálózatát adná vissza, és nem *Gracie*-t, vagyis a jobb oldalt. Ezenkívül az `auto` kapcsolót `start` helyett `add`-re kell állítani, mert *George* kiszolgálóként működik: csak készen kell állnia *Gracie* számára, hogy az alagutat működésbe helyezze.

Az alagút elindítása és kipróbálása

Most ugrik a majom a vízbe! Előbb *George*-on, majd *Gracie*-n adjuk ki a következő parancsot:

```
ipsec setup restart
```

George végigolvassa a */etc/ipsec.conf* állományt, betölti a `george-gracie` alagút-meghatározást, és felkészül a kapcsolatok fogadására. *Gracie* ugyanezt fogja tenni, és felélesztí az alagutat. Az indulással kapcsolatos üzenetek naplózása a */var/log/messages* vagy a */var/log/secure* állományokba történik. Amennyiben az ügyfélrendszeren `ipsec setup restart` parancs kimenete az „IPSec SA established” üzenettel ér véget, az alagút működésre kész!
Próbáld pingelni a távoli hálózat gépeit, vagy kísérelj meg valamilyen más módon kapcsolódni hozzájuk – a kapcsolatnak nem szabad különböznie az alagút üzembe helyezése előtt tapasztalt működéstől!

A `tcpdump` futtatásával hasznos lehet meggyőződni arról, hogy a kártyán kizárólag ESP- (Encapsulating Security Payload) csomagok közlekednek, és nem tényleges ping, FTP-, vagy egyéb csomagok vannak kiküldve.
A következő hónapban egy-két újabb forgatókönyvet fogunk áttekinteni, és még jobban elmélyedünk a FreeS/WAN gyönyörűséges rejtelmeiben.
Remélem, írásom elegendő útbaigazítást nyújtott a biztonságos vezeték nélküli hálózathasználat megkezdéséhez.

Linux Journal 2003. január, 105. szám

Mick Bauer (mick@visi.com)
Hálózati biztonsági tanácsadó az Upstream Solutions Inc.-nél Minneapolisban (Minnesota). Mick a szerzője a hamarosan megjelenő új O'Reilly könyvnek, amelynek címe „Building Secure With Linux”.

KAPCSOLÓDÓ CÍMEK

A FreeS/WAN honlapja ➲ http://www.freeswan.org/
FreeS/WAN-levelezőlista ➲ users@lists.freeswan.org
FreeS/WAN-cikk a SysAdmin-on
➲ http://www.samag.com/documents/s=1159/sam0011i/0011i.htm