VPN-átjáró telepítése

Hogyan kell telepíteni és üzemeltetni IPSec-alapú tűzfallal ellátott VPN-átjárót mindössze egyetlen rendszerindításra alkalmas hajlékonylemezre telepített Linux-változattal?

A VPN olyan eszköz, amely lehetővé teszi az adatok biztonságos átvitelét még az olyan megbízhatatlan hálózatokon is, mint amilyen az Internet. A VPN-t gyakran arra használják, hogy helyi hálózatokat (LAN) az Internet révén széles körű, vagyis nagy kiterjedésű hálózattá (WAN) egyesítsenek. Lehetséges, hogy két iroda között VPN-t kell kiépítenie, de arról már nincs meggyőződve, hogy a vállalati szintű VPN-megoldásokkal együtt járó magas kialakítási költségek is indokoltak-e.

A LAN-ok számára tervezett alkalmazások – amelyek például a hálózati állománymegosztást használják – működése a WAN-csatlakozást követően alapvetően leértékelődik. Hasonlóképp a WAN-kapcsolatok sávszélessége és hosszabb válaszideje kedvezőtlenül befolyásolja a megbízhatóságot, a csoportkezelést és a vékonyügyfélprogram működését. Ezenkívül lehet, hogy Ön otthonról, a dolgozószobájából szeretne nagy sebességű internetelérése révén zökkenőmentesen és biztonságosan kapcsolódni cége belső hálózatához, IPSec-útválasztón keresztül. De lehet, hogy éppen csak érdeklődik a VPN és az IPSec iránt és szeretné őket kipróbálni – cikkünk Önnek szól.

Írásunkban bemutatott VPN-tűzfalak képesek bármilyen 486-os vagy annál erősebb számítógépen működni, amelybe 16 MB vagy annál több memóriát, valamint kettő, Linuxszal együttműködő ethernet hálózati kártyát építettek.

Alapgondolatom az volt, hogy a felhasználók kezébe olyan kiindulópontot adjunk, amellyel egyedüli, önálló csomagból mindenki készíthet magának nagyméretű, biztonságos, méretezhető és pontosan beállítható VPN-eket, amelyek ráadásul más közönséges, kereskedelmi forgalomban kapható VPN-ekkel is képesek együttműködni. Ha kevés karbantartást igénylő tűzfal–VPN-átjáróval kíván kísérletezni, az itt bemutatásra kerülő programcsomag eszményi lehet az Ön számára. Jelen írásunkban azt mutatjuk be, hogyan telepítsünk a legkevesebb költséggel VPN-átjárót, amely az IETF (Internet Engineering Task Force) IPSec ajánlását használja.

Az IPSec olyan nyílt szabvány, amelyet szinte minden ismertebb tűzfalprogram és alkatrészgyártó, mint például a Lucent, a Cisco, a Nortel és a Check Point támogat. Ez a csomag széles körű együttműködésre képes IPSec-et tartalmaz, amely valódi 3DES-titkosítást és MD5-hitelesítést használ a végpont-webhely, illetve a végpont-végpont jellegű VPN-ekben. Mindezt jó lenne úgy megvalósítani, hogy ne kelljen teljes Linux-változatot igénybe venni, vagy az IPSec-modult befordítani a rendszermagba.

Az általunk itt megvizsgált VPN a FreeS/WAN-en alapul (➲ http://www.freeswan.org), amely az IPSec-ajánlás nyílt forrású, hordozható megvalósítása. Bemutatták, hogy a FreeS/WAN különböző mértékű együttműködésre képes a Cisco IOS 12.0 és az annál fejlettebb útválasztókkal, Nortel Contivity kapcsolókkal, OpenBSD, Raptor Firewall tűzfallal, Check Point FW-1, SSH Sentinel VPN 1.1, F-Secure VPN, Xedia Access Point, PGP 6.5/PGPnet és későbbi változatokkal, IRE SafeNet/SoftPK, Freegate 1.3, Borderware 6.0, TimeStep PERMIT/Gate 2520, Intel Shiva LanRover, Sun Solaris és Windows 2000 rendszerekkel.

A FreeS/WAN hivatalos honlapján megfelelési listáját a Világhálón elérhető leírással együtt rendszeresen frissíti. A letölthető csomagban a FreeS/WAN 1.5 változata szerepel. A Linux Router Project (➲ http://www.linuxrouter.org) alapján összeállítottam egy egyetlen hajlékonylemezből álló változatot, amely a tűzfal alapbeállításait telepíti. A tömör Linux-változat egyetlen rendszerindításra alkalmas hajlékonylemezen elfér. Ez a lemez tulajdonképpen ***Charles Steinkuehler*** Eiger-lemez képállománya, Steinkuehler által készített IPSec-megfelelő rendszermaggal és az LRP IPSec programjával együtt.

A tűzfal kiépítéséhez a Linux-változatokban megtalálható IP Chains programot használtam. A felhasznált változat a 2.2.16 Linux-rendszermagra épül és a DUCLING mozaikszavas elnevezést kapta, tehát Diskette-based Ultra Compact IPSec Gateway (hajlékonylemez-alapú ultratömör IPSec-átjáró).

A tömör Linux-változatok kanyargós utat jártak be. Szakmai szempontból az LRP ***Dave Cinege*** tömör változatára hivatkozik. Több változat is forgalomban van, beleértve ***Matthew Grant*** immár „halott" Eiger-változatának Charles Steinkuehler által készített újabb változatát (EigerStein). További hasonló változat a ***David Douthitt*** által készített Oxygen (➲ http://leaf.sourceforge.net/content.php?menu=900&page_in=1). A fentieken kívül létezik még a LEAF-vállalkozás (Linux Embedded Appliance Firewall), amely ernyő módjára fogja össze a programfejlesztőket, és megkísérli összehangolni a programkibocsátásokat és -leírásokat, vagyis afféle „mindent egy helyen beszerzési hely" a tömör Linux-változatok számára (➲ http://leaf.sourceforge.net). A továbbiakban az LRP mozaikszót használom az alább bemutatott tömör Linux-változatra való hivatkozáshoz, annak ellenére, hogy sokan talán helytelennek találják az elnevezést.

Amennyiben MS Windows 9x rendszert használ, az önkibontó állomány a kicsomagolás után egy szabványos, nagy sűrűségű hajlékonylemezre telepíti magát. De Linux alatt a képállományt rendszerindításra alkalmas hajlékonylemezre is rá lehet másolni. Amint a lemez elkészült, indítsuk el róla a rendszert, majd végezzük el a beállítási állományok szerkesztését. Ezzel a munka el is van végezve: nincs szükség a lemezfelosztások formázására vagy a merevlemezre telepített betöltéskezelő programokkal való bogarászásra. Amennyiben mégsem lenne elégedett az eredménnyel, távolítsa el a hajlékonylemezt a meghajtóból és indítsa újra a gépet.

Keresse fel az alábbi helyet a Világhálón:
➲ http://leaf.sourceforge.net/devel/thc, ahol bővebben olvashat a lehetőségekről.

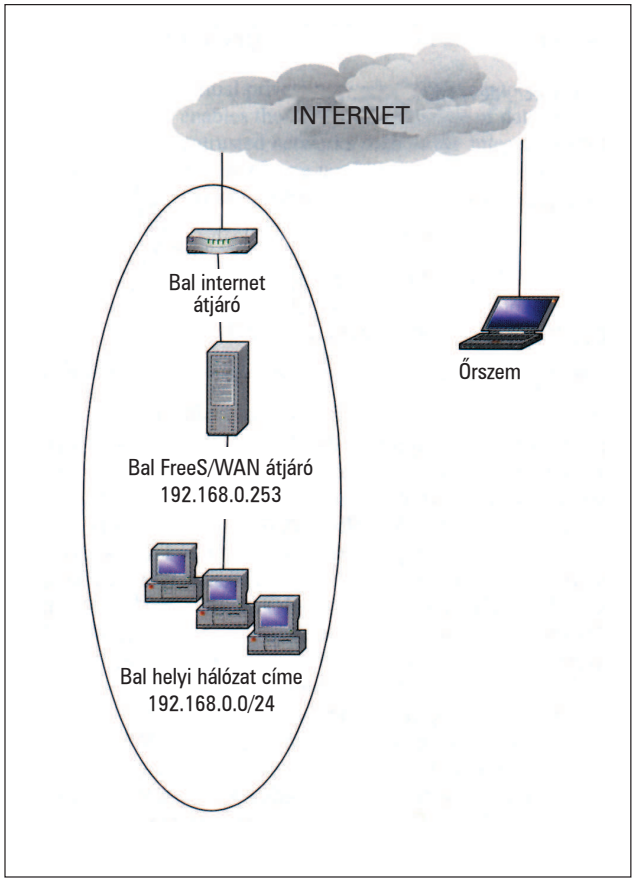
Háttérműveletek a tűzfalon és a VPN-ben

Az LRP itt bemutatott változata szabványos IP Chains-alapú tűzfalra épül. Az IP Chains (a 2.4.x sorozatú rendszermagban már IP Tables) szabadon terjeszthető csomagszűrő Linux-rendszerekhez (lásd még ***David A. Bandel*** A Netfilter

megszelídítése című írását a Linuxvilág 2001. októberi számának. Sokat lehet tanulni az IP Chains HOGYAN-oldalairól is, amennyiben valaki még járatlan e tűzfalkezelő eszköz beállításában. Ez utóbbi leírást a
➲ http://www.Linuxdoc.org/HOWTO/ipchains-howto/html
címen olvashatja el). A VPN IPSec-megvalósítását a FreeS/WAN készítette el, amely megfelel az IETF IPSec-ajánlásának. Az IPSec tulajdonképpen az Internet Protocol (IP) kiterjesztése, amely gondoskodik a hitelesítésről és a titkosításról. Ez utóbbi két feladatot három protokoll látja el, nevezetesen az ESP (Encapsulated Security Payload), az AH (Authentication Header) és az IKE (the Internet Key Exchange). Valamennyi rendszeralkotó szerepel a FreeS/WAN IPSec-megvalósításában és általában átlátható a végfelhasználók számára. Az ESP és az AH protokoll kezeli a titkosítási és hitelesítési feladatokat, az IKE pedig a kapcsolati jellemzőket közvetíti, többek között a kezdeti jellemzők beállítását, a titkosítási kulcsok kezelését és megújítását. Jelenleg a FreeS/WAN egyetlen titkosítási sémát támogat, a „triple Data Encryption Standard"-szabványt, azaz rövidítve a 3DES-szabványt – amely jelenleg *a* Szabvány az IPSec-titkosításban.
A hitelesítés az úgynevezett megosztott titkokból (megosztott kulcs) készült MD5-kivonat alapján történik. A megosztott kulcsok lehetnek kölcsönösen elfogadott jelsorozatok, RSA titkosítási kulcspárok vagy X.509 igazolások, illetve nyugták. A FreeS/WAN KLIPS (kernel ipsec, vagyis a rendszermagba fordított IPSec-modul) üzembe helyezi az AH és ESP protokollokat, valamint a csomagok kezelését. Az IKE-folyamatok kezelik a kulcsegyeztetéseket, a kulcsfrissítéseket pedig a FreeS/WAN önállóan működni képes `pluto` démonja végzi.

Rendszerigények és telepítés

A telepítés megkezdéséhez mindenek előtt egy hajlékonylemez-meghajtóval – jómagam csak 3,5 hüvelykes hajlékonylemez-meghajtókat használtam – ellátott számítógépre lesz szükség, amelybe két hálózati kártyát is építettek. Az LRP Linux-változat telepítési igényei csekélyek, nem szükséges hozzá erőteljes gép. A célnak bármilyen Intel 486-os vagy annál erősebb gép megfelel, amelybe 8 MB vagy annál nagyobb memóriát építettek.
A munkához szükséges két hajlékonylemez, amelyeknek megbízható, nagy sűrűségű lemezeknek kell lenniük, de akár lehetnek például az AOL reklámhordozó lemezei is. Soha semmilyen gondom nem akadt a megszokott (generic) hajlékonylemez-meghajtókkal, viszont az Imation USB U2 SuperDisk-meghajtójával a hajlékonylemez formázása során előfordultak írási hibák.
Töltsük le a megfelelő ***DUCLING.tgz/zip***-változatot az
➲ ftp://ftp.cinemage.com/pub webhelyről, majd csomagoljuk ki az állomány tartalmát. Ha a gépe állandó IP-címmel van ellátva, töltse le az állandó változatot, ellenben dinamikus IP-cím esetén a DHCP-változatra lesz szüksége. Ha a gépén Windows 9x rendszert használ, töltse le a ***ducling-stat-W9x-1-0.zip*** vagy a ***ducling-dyn-W9x-1-0.zip*** állományt. A tömörített állomány WinZippel való kibontását követően létre fog jönni a ***ducling-stat-1-0.exe***, illetve a ***ducling-dyn-1-0.exe*** állomány, valamint a könyvtári modulok. Az ***.exe*** önkicsomagoló állomány, amely a hajlékonylemezt formázza, majd felírja rá a képállományt (image). Futtassa a ***ducling-stat-1-0.exe*** vagy a ***ducling-dyn-1-0.exe*** programot és helyezzen egy hajlékonylemezt a meghajtóba. Ne felejtse el, hogy a lemezen lévő összes adat el fog veszni.
Abban az esetben, hogy ha Ön MS-DOS-t vagy Windows 3.1-et használ, először az állandóan a memóriában tartózkodó `FDREAD.EXE` segédprogramot kell a DOS-ba betölteni, ha 1722 KB formátumú hajlékonylemezre kíván írni, illetve ilyenről olvasni. Az `FDREAD.EXE` ***Christopher H. Hochstätter*** ingyenes segédprogramja. Ha számítógépén Linuxot használ, töltse le a fent említett állományokat, majd a `tar` programmal végezze el az állományok kicsomagolását. Az alábbi



A webhely gyalogos beállítása

példában DHCP-megfelelő, dinamikus címfeloldást támogató programot mutatunk be:

```
tar xvfz ducling-dyn-1-0.tgz
```

Ezután írjuk fel a ***ducling-dyn-1-0.img*** képállományt a formázott hajlékonylemezre a Linux `fdformat`, illetve `dd` parancsai segítségével:

```
fdformat /dev/fd0u1722
dd if= ducling-dyn-1-0.ima of=/dev/fd0u1722
```

Ha a Linux a hajlékonylemez létrehozását a fent leírt módon elvégezte, máris rendelkezik egy rendszerindításra használható lemezzel. A ***zipfile/mappa*** nevű modulok tartalmazzák a hálózati kártyák meghajtómoduljait a tűzfalmaszkoláshoz szükséges kiegészítő modulokkal együtt. Másolja a ***zipfile/mappa*** tartalmát egy további MS-DOS formátumúra formázott hajlékonylemezre mostani bemutatónk beállításához (lásd alább). Linuxban ezt az alábbi két paranccsal tehetjük meg:

```
fdformat /dev/fd0
```

ezután pedig

```
mkdosfs /dev/fd0
```

A `mount` paranccsal tegyük a hajlékonylemezt a rendszer számára hozzáférhetővé, és másoljuk át a modulokat. Olvassa el a ***README*** állományban mellékelt leírást, amely a tűzfal, illetve útválasztó beállításának részleteit tartalmazza. Amennyiben az összes kívánt csomagot kapacitáshiány miatt nem lehet egyetlen hajlékonylemezre összesűríteni, meg kell vizsgálni a két hajlékonylemezes telepítés lehetőségét – a DUCLING-változat README-állományából erről is kaphatunk tájékoztatást – azonban a betölthető CD-ROM avagy kicsi merevlemez elkészítésének leírását is megtalálhatjuk. Bővebb tájékoztatás végett keresse fel az LRP-leírásnak a Világhálóra feltett oldalait.

Az LRP rendszerindító hajlékonylemezek – a meglepő igazság

Talán meglepődik azon, hogy az LRP DOS-formátumú hajlékonylemezeket használ. Valószínűleg még jobban meglepődik, amikor felfedezi, hogy DUCLING-változat 1722 KB-os képállományként telepíti magát a lemezre. A 3,5 hüvelykes, nagy írássűrűségű hajlékonylemez műszakilag 2 MB kapacitású adathordozó, s ezt adatot a lemezen is feltüntetik: 2 MB „nyers" vagyis formázatlan kapacitás. Az 1440 KB-os formázott tárolókapacitás csupán a hagyományos lemezformátum eredménye, amelyben az adathordozóra 80 sávot írnak fel és 18 szektort sávonként. Megfelelő eszközökkel olyan hajlékonylemezeket hozhatunk létre, amelyeken 80 szektor és szektoronként 24 sáv van kijelölve, ez összesen 1920 KB-os kapacitást jelent. Az LRP-változatokhoz általában 1680 KB-os formátumú hajlékonylemezeket használnak és a sávfelírás biztonságosnak tűnik. A fentebb említett formátumokon kívül az 1722 KB (82, 21), 1743 (83, 21), és 1760 (80, 22) lemezformátumokat is használják. Az 1722 KB-os lemezformátumot a próbák során elég megbízhatónak találtam, és mindeddig nem tapasztaltam olyan hibákat, amelyekről beszámolhatnék. Egészen 1920 KB-os méretig hoztam létre és használtam nagy kapacitásúra formázott hajlékonylemezeket. A szokásosnál nagyobb kapacitásúra formázott hajlékonylemezek hajlamosak alkalmatlanná válni a rendszerindításra, nyilvánvalóan a számítógépek BIOS-a és a lemezen lévő szabványostól eltérő szektorméret ellentétéből fakadóan. Állítólag az 1680 KB-nál nagyobb kapacitású lemezek akár alkatrészfüggőségi gondoktól is szenvedhetnek. A Windows NT és a Windows 2000 rendszerekről az a hír járja, hogy az 1680 KB-nál nagyobb kapacitású lemezeknél a lemezre történő írás során megbízhatósági gondok jelentkeznek. Az MS Windows 9x operációs rendszerek az alapértelmezésnek megfelelő beállítások megváltoztatása nélkül képesek a hajlékonylemezt a szokásosnál nagyobb kapacitásúra formázni. Linux-rendszerekben gyakran szükséges, hogy a `mount` parancs kiadásakor a tényleges formátumot is megjelöljük, vagyis például `/dev/fd0u1722`, ahol az `fd0` a 0 (nullás) hajlékonylemez-meghajtót jelöli, míg az `u1722` az 1722 KB-os lemezformátumot. A Linux szabványos hajlékonylemez-meghajtója az alapértelmezés szerint `/dev/fd0u1440`, tehát 1440 KB-os formátumú. A nagy kapacitású lemezek készítésével és ilyenek használatával kapcsolatos tanácsok végett tanulmányozza a ***Paul Batozech*** készítette LRP-rendszerindító lemez HOGYAN-leírását. Szóban forgó témánkon túl számos

A FreeS/WAN telepítési kapcsolat listája

```
conn Listing for the Setup Shown in Figure 1
conn sentinel-vpn
       type=tunnel
#BiztonsÆgi Ætjær , amely m g tt hÆl zat van
#a k vetkezı ugrÆs errefelØ van.
   type=tunnel
   left=1.2.3.4
   leftnexthop=1.2.3.5
   leftsubnet=192.168.0.0/24
   right=0.0.0.0
        rightnexthop=
        rightsubnet=
        keyexchange=ike
         keylife=8h
         keyingtries=0
         pfs=no
         authby=secret
         auto=add
```

más érdekességre is bukkanhat a ➲ http://leaf.sourceforge.net/devel/thc címen. Az MS Windowshoz ***Gilles Vollant*** készítette el a WinImage-et (➲ http://www.winimage.com), amit különösen hasznosnak és felhasználóbarátnak találtam.

Az olyan Linux-eszközökhöz képest azonban, mint amilyen az `fdformat`, `mkdosfs` és a frissebb szuperformázó-alkalmazások, ez több szempontból is korlátozott program. Az itt vizsgált, MS Windows számára létrehozott önkicsomagoló állományok a WinImage program segítségével készültek.

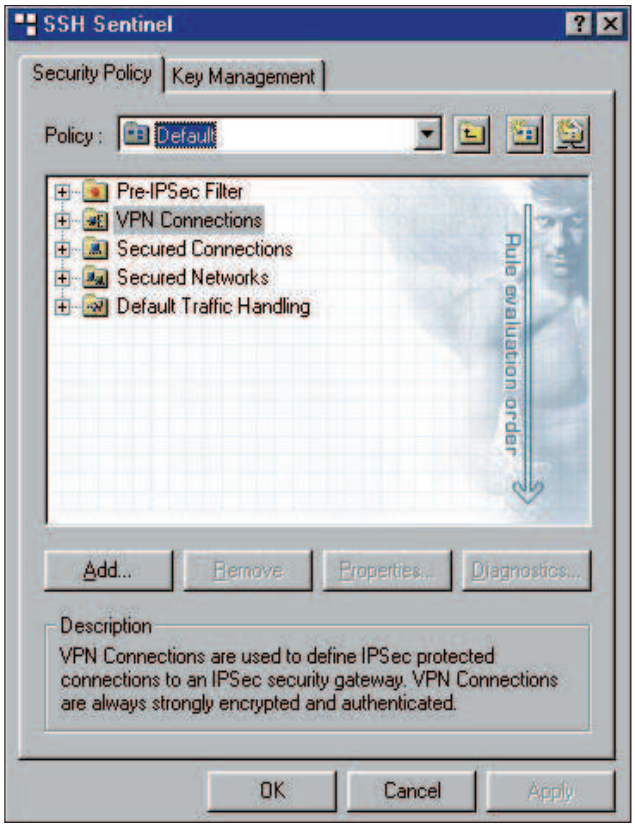
Hogyan történik az LRP-változat betöltése?

Mielőtt elkezdene dolgozni az LRP-vel, hasznos megfigyelni, hogyan is működik a rendszer. Ha a rendszerindító lemezt veszi szemügyre, egy sor állományt fog látni: ***ldLinux.sys***, ***Linux***, ***sysLinux.cfg***, ***root.lrp***, ***modules.lrp***, és a ***local.lrp*** nevű állományt.

Az ***ldlinux.sys*** tölti be a csizmahúzó szerepét, vagyis ez az az állomány, amely gondoskodik a rendszermag – a Linux nevű állomány – és a kezdeti ***root.lrp*** csomag memóriába töltéséről. A rendszermag megkezdi működését, létrehoz egy ramlemezt és ide bontja ki a ***root.lrp*** állományt. A ramlemez ezúttal nem más, mint egy tárterület, amelyet a program lemezrészként foglal le. Más szóval a rendszermag ezután teszi elérhetővé a `mount` paranccsal a ***sysLinux.cfg***-ben meghatározott rendszerindító készüléket. Az indítólemezen levő maradék ***.lrp***-csomagok kibontása a ***syslinux.cfg*** állományban előírtaknak megfelelően történik, majd azok is betöltődnek a ramlemez területére.

Az ***.lrp***-csomagok szabványos Unix-típusú ***tar***-állományok, vagyis `tar` és `gzip` programmal tömörített archívumok. Ha az ***.lrp***-csomagok már telepítve vannak a ramlemez könyvtárfájába, a rendszer megkezdi a betöltési folyamatot a szabványos Linux ***rc***-állományban meghatározott betöltési sorrendnek megfelelően.

Az LRP egyszerűen szólva maga a lecsupaszított rendszermag betölthető modulokkal és egyéb ***.lrp*** formátumba csomagolt programokkal együtt. Az LRP valódi Linux; általában véve, ami képes működni közönséges Linux-rendszeren, az bizonyosan képes lesz az LRP-lemezről is elindulni.



1. kép A Sentinel Biztonsági házirend

Gyakran az LRP-alkalmazások és -szolgáltatások kiterjesztésének akadálya a hajlékonylemez szabta méretkorlát. Amennyiben Ön további szolgáltatásokat igényel, például távoli felügyeletet SSH-n keresztül, DNS-kiszolgálót és egyebeket, talán a több hajlékonylemezes, CD-ROM-alapú, vagy teljes merevlemezt igénylő változatot is meg szeretné majd tekinteni.

VPN-útválasztó, illetve tűzfal telepítése és beállítása

A rendszerindító hajlékonylemez létrehozása után győződjön meg róla, hogy a hajlékonylemez be lett-e abba a számítógépbe helyezve, amelyiken a VPN-tűzfalat üzemeltetni kívánja. Ellenőrizze, hogy a rendszerindítás hajlékonylemezről történik-e. A VPN-tűzfal indításakor a gép képernyőjén meg fogja látni az LRP üdvözlőképernyőjét, a Linux betöltőprogram üzeneteit, majd a bejelentkező parancsot.

Ha eddig eljutott, gratulálunk! Sikeresen telepített egy LRP-változatot. Most már elkezdheti beállítani az LRP-tűzfal jellemzőit úgy, ahogyan az a programhoz mellékelt leírásban is szerepel. A tűzfal beállítása után a VPN-t is be kell állítani. A programhoz járó DUCLING-leírás megadja a részhálózat-részhálózat beállításának részleteit. Ebben a leírásban található az IPSec hitelesítési módjának beállítása (***/etc/ipsec.secrets***), az IPSec-hálózat beállítása (***/etc/ipsec.conf***), és a tűzfal az 500-as kapura (UDP), illetve az 50 és 51-es kapura vonatkozó hozzáférés engedélyezési szabályokkal együtt.

Fontos megjegyezni, hogy nem szükséges állandó IP-cím a VPN-kapcsolatok használatához. A „gyalogos" beállítást a következő fejezetben mutatjuk be, ahol a VPN-ügyfél nem meghatározott állandó IP-címmel rendelkezik. Működtettem VPN-eket dinamikusan kiosztott IP-címekkel ellátott géppárok között. A DHCP által a gépekhez rendelt IP-címes VPN-ek kezelése akkor válik bonyolulttá, ha mindkét kiosztott IP-cím gyakran változik meg. A következő fejezet a „gyalogos" beállítás lehetőségeit mutatja be a DUCLING- és Microsoft-alapú IPSec-ügyfél között.

Példa az együttműködésre

Az alábbi példánk az MS Windows 9x, illetve 2000 ügyfélprogram által létesített végpont-webhely kapcsolatot mutatja be, amely az SSH Communication Sentinel 1.1 (nyilvános béta3-változat) nevű programot használja. A FreeS/WAN az IPSec-megvalósítások bő választékával képes együttműködni. A telepítési folyamat bonyolultsága és a számítási teljesítmény nagysága termékenként változik.

Számos 3DES-, illetve MD5-titkosítást támogató termék az IKÉ-n keresztül képes együttműködni a FreeS/WAN-nel. Másrészt arra a megállapításra jutottam, hogy az erős titkosítást támogató, összes tulajdonsággal rendelkező IPSec-megvalósítások jogtiszta beszerzése roppant fárasztó, különösen akkor, ha Ön, az olvasó, az Egyesült Államokon kívül él.

Számos alkatrészgyártó kínál IPSec-megoldásában korlátozott lehetőségeket. Például az egyik termék csak a gyenge titkosítást támogatja, a másik pedig esetleg a VPN-szolgáltatásokat a szállításra korlátozza. Fontos az IPSec-en keresztül biztosított két VPN-üzemmód megkülönböztetése: a továbbítási és alagút üzemmódé. Továbbítási szállítási feladatokat lát el és hitelesítést végez a két végpont között. Az alagút üzemmód inkább részhálózatok összekapcsolására használható és lehetővé teszi a részhálózatok elérését a tűzfalon és útválasztón keresztül. Alapjában véve a továbbítási mód a forgalmat a végpont-végpont közötti kapcsolattartásra korlátozza. Az alagút üzemmód megengedi a végpont-végpont, végpont-részhálózat és részhálózat-részhálózat adatcseretípusokat.

Úgy tűnik, létezik legalább egy alkatrészgyártó, amelyik nem engedi meg, hogy IPSec-megoldása állandó IP-című kapcsolatra fusson. Úgy látszik, hogy az SSH Sentinel termék (➲ http://www.ipsec.com) egyik fentebb említett gondtól sem szenved, valószínűleg abból a tényből fakadóan, hogy a cég székhelye az Egyesült Államokon kívül van.

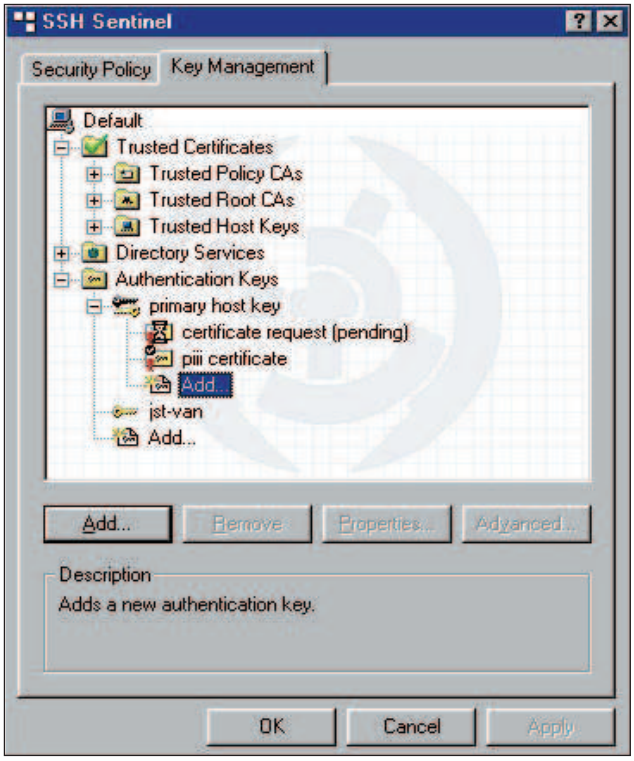
Letöltöttem és kipróbáltam a Sentinel 1.1 beta3 harmincnapos próbaváltozatát, és a Windows 98-cal működő asztali számítógépen nagyon könnyűnek találtam a beállítását. A Sentinel leírása a FreeS/WAN VPN-átjáróval kapcsolatos beállítási példákat is tartalmaz.

Az alábbiakban olvasható a „gyalogos beállítás" összefoglalója, amely dinamikusan kiosztott IP-címmel rendelkező távoli felhasználók számára lehetővé teszi, hogy csatlakozzanak a tűzfal mögötti helyi hálózathoz.

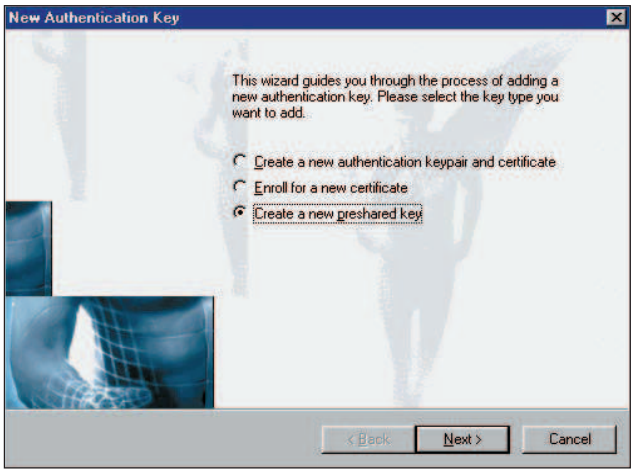
Szükség lesz az 50 és 51-es kapu (TCP) és az 500-as kapu (UDP) megnyitására a dinamikus IP-cím, illetve az internetszolgáltató DHCP-címtartománya számára. *Ábránkon* (35. oldal) az alapvető telepítést láthatjuk. Szükség lesz a DUCLING FreeS/WAN tűzfalon a ***/etc/network.conf*** állomány szerkesztésére: lépjen be az ***lrcfg***-be, válassza az egymás után következő menükben mindig az első pontot, végül a beállítást:

```
eth0_IP_SPOOF=NO/
```

az alagút üzemmódba irányított csomagok letiltásának kikapcsolásához. A programhoz mellékelt leírás részletes útmutatással szolgál arra nézve, hogyan kell ezeket a feladatokat elvégezni. A FreeS/WAN ***ipsec.conf*** állományának tartalmát a *listánkon* tekinthetik meg. Az ide vonatkozó ***ipsec.secrets*** állományban pedig az alábbi bejegyzés szerepel:



2. kép Új kulcs hozzáadása

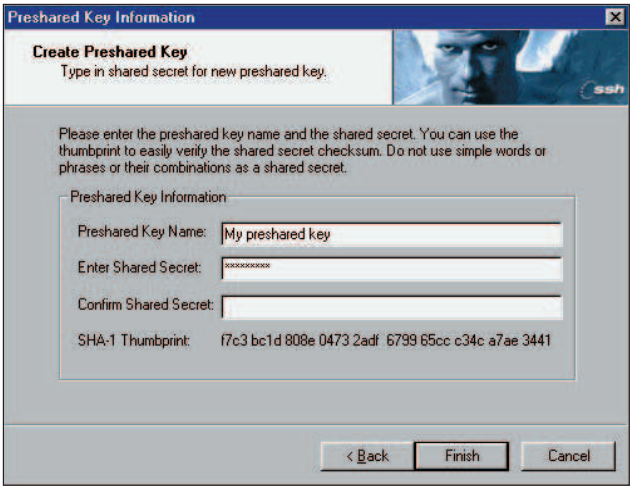


3. kép Előre megosztott kulcs beállítása

```
1.2.3.4  0.0.0.0  :PSK Ide kell  rni a
gyalogos beÆll tÆs jelszavÆt
```

ahol az idézőjelek között megadott jelsorozat a megosztott titok jelkombinációja. A 0.0.0.0 formában megadott IP-cím bármilyen IP-címet jelölhet, a `rightsubnet` és a `rightnexthop` értékek üresen hagyása végpont–részhálózat-típusú kapcsolatra utal. A Sentinel IPSec-szolgáltatás üzembe helyezéséhez az alábbiakat kell elvégezni:

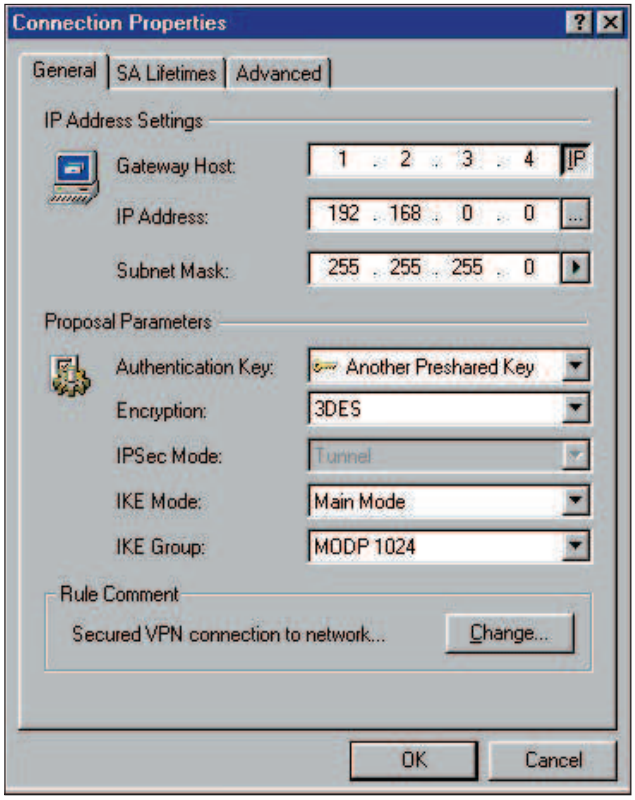
1. Töltse le az SSH Sentinel programot a ➲ http://www.ipsec.com címről, és a telepítés során kövesse az útmutatóban leírtakat.
2. Lépjen be a Sentinel program ***Sentinel Policy Manager***-be (házirend-kezelőjébe): lásd a *1. képet*.



4. kép „Megosztott titok" begépelése

5. kép Kulcs begépelése

3. Válassza a ***Key management*** fület (Kulcskezelés) és a ***Authentication*** keys (Hitelesítő kulcsokat), majd nyomja meg az ***Add*** (Hozzáadás gombot): a miként *2. kép* mutatja.
4. Hozzon létre új, előre megosztott kulcsot (***Create***), majd bökjön rá a ***Next*** (Következő) gombra (*3. kép*).
5. Gépelje be saját előre megosztott kulcsát – idézőjelek nélkül. Ennek meg kell egyeznie a megosztott titok jelsorozattal, amelyet a */etc/ipsec.conf*-ban adott meg (*4. kép*).
6. Nyomja meg a kész gombot.
7. Az SSH Sentinel házirend-kezelője főkonzolának Biztonsági házirend menüjében válassza a VPN-kapcsolatokat, azon belül pedig az ***Add***-ot (Hozzáadás).
8. Gépelje be a távoli átjáró IP-címét és nevét: példánkban ez 1.2.3.4, és válassza az előzetesen megosztott „titkot", amelyet hitelesítési kulcsként az ötödik lépésben hozott létre (*5. kép*).
9. Válassza a 3DES-titkosítást: a ***Main mode*** (Fő üzemmódot) és a ***MODP 1024***-et az IKE-üzemmód és az IKE-csoport számára.
10. Állítsa be az IKE élettartamát, vagyis az ismételt kulcskiosztások közötti időszak hosszát ugyanarra az értékre, amely az ***ipsec.conf*** állományban szerepel; ez általában 480 perc, azaz 8 óra.



6. kép A „Properties" (Tulajdonságok) menüfül a VPN-kapcsolatoknál

Mentsen minden beállítást és próbáljon meg pingelni egy tűzfal mögötti gépet, vagyis próbálja ki a belső csatlakozófelületet, a 192.168.x.254-es címet. Ekkor a kapcsolatnak létre kell jönnie. Próbálja futtatni a Sentinel hibakereső programját, hogy azzal ellenőrizze, a kapcsolat valóban létrejött-e. Meg kellett állapítanom, hogy a hibakereső program néha előidézheti a FeeeS/WAN–Windows-kapcsolat meghibásodását. Amennyiben ez történik, a FreeS/WAN-átjárón indítsa újra az IPSec-et és élessze fel az egyes kapcsolatokat. Itt hadd hívjuk fel ismét a figyelmet arra, hogyha a kapcsolatot újra kell indítania, az LRP-t futtató gépbe jelentkezzen be és az IPSec-elemek újraindításához írja be:

```
#etc/initd.d/ipsec restart
```

Úgy találtam, hogy a Windows 2000 Professionalban – de a Windows 98-ban nem – az útválasztó táblát a DOS-konzolból a megosztott részhálózatra kézzel kell módosítani:

```
route ADD 192.168.0.0 MASK 255.255.255.0 1.2.3.4
```

Ellenőrizze a Microsoft `route` parancsát a leírásban.

Összefoglalás

Jelen cikkünk egyetlen 3,5 hüvelykes hajlékonylemezről indított tűzfalas VPN-átjáró kialakításának eszközeit vázolja fel. Mindössze egyetlen hajlékonylemez révén adott a lehetőség, hogy számítógépeket és változatos elrendezésű hálózatokat az Internet segítségével biztonságosan kapcsoljunk össze.
A DUCLING-változat a vázig lecsupaszított Linux-változat. Amennyiben meggyőződött arról, hogy a FreeS/WAN VPN valóban képes az igényeinek megfelelni, akkor vagy egy

A leaf honlapja

teljesebb LRP-változatot választ, vagy egy teljes Linux-változatot választ olyan feladatok megoldására, mint amilyen például a távoli elérés, a biztonságos héjprogram, az SSH vagy a DNS-kiszolgáló.

Duncan Napier
vezeti a kanadai North Vancouverben (British Columbia) a Napier System Research vállalkozást, amely hálózati és informatikai tanácsadással foglalkozik.

Kapcsolódó címek a hibakereséshez

Az LRP beállításával kapcsolatos gondok megoldása végett keresse fel a SourceForge LRP webhelyét ➲ http://leaf.sourceforge.net. *Richard Onanian* honlapja a ➲ http://leaf.sourceforge.net/devel/thc a hibakereső adatok és HOGYAN-ok szempontjából hasznos. Ha a hibakeresést a FreeS/WAN-nál kell végezni, akkor tanulmányozza a termék leírását a ➲ http://www.freeswan.org címen.
Amennyiben a kérdéseire nem kapna kielégítő választ a fentebb említett forrásokból, vizsgálja át a LEAF ➲ http://www.geocrawler.com/lists/3/SourceForge/7325/0 és az LRP ➲ http://www.geocrawler.com/lists/ 3/Linux/303/0 levelezési listák archívumait.
Ha a gondja közvetlenül a FreeS/WAN VPN-nel kapcsolatos, akkor a FreeS/WAN archívumait olvasgassa ➲ http://lists.freeswan.org/mailman/listinfo.
Amennyiben az említett gond még mindig makacsul ellenáll a megoldási kísérleteknek, küldje el őket a megfelelő levelezési listákra.