A Firewall Builder használata (2. rész)

A bástyagép beállítása és az IP Tables tűzfalszabályainak megadása után már tisztán láthatjuk a biztonsági házirend lényegét.

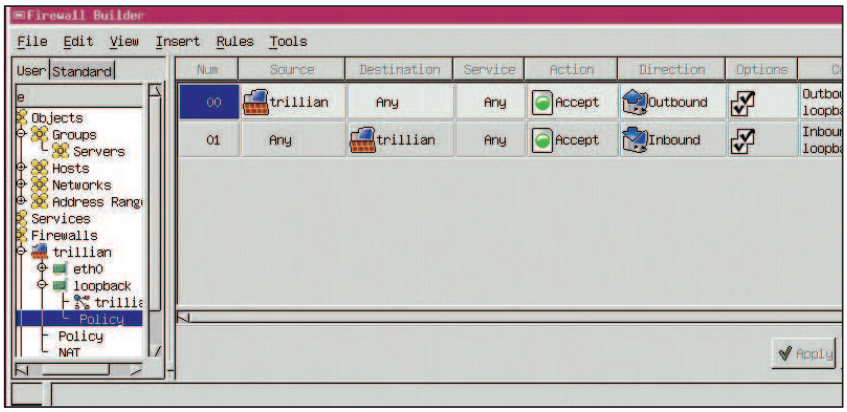
A múlt alkalommal a Firewall Builderben elkészítettük azokat az újrafelhasználható objektumokat, amelyeket az IP Tables-szabályokban fogunk alkalmazni. Ez alkalommal két szabálykészletet fogunk a Firewall Builder segítségével létrehozni: az egyik a bástyagép számára készül el, amelynek önmagát kell megvédenie, a másik egy tűzfal számára, amelynek egy teljes hálózat biztonságáról kell gondoskodnia.

Helyi szabályok a bástyagépen

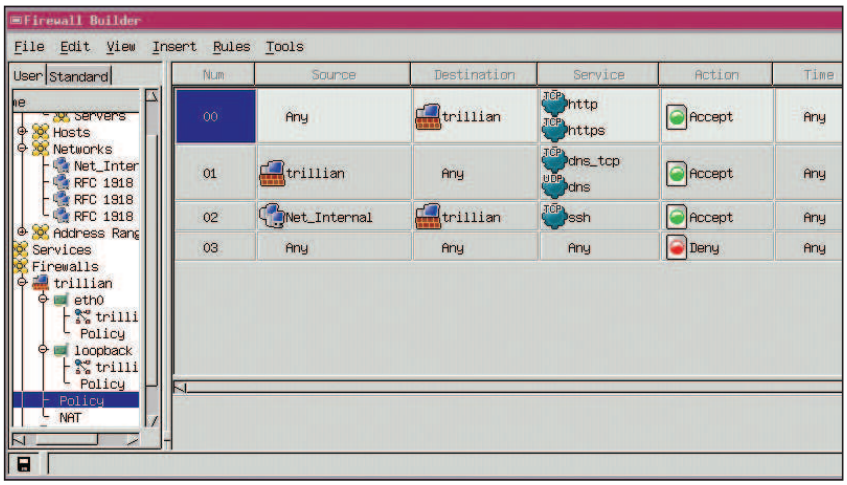
Elsőként tekintsük át a bástyagép helyzetét. A Netfilter/IP Tables, illetve általában a csomagszűrés kapcsán széles körben elterjedt tévhit, hogy a csomagszűrés kizárólag a tűzfalak feladata. Ha valóban biztonságos rendszert szeretnél, elég balga ötlet volna a biztonságot egyetlen elemre bízni. Természetesen szükség van egy gondosan beállított és felügyelt tűzfalra, ami az összes hálózatra csatlakozó számítógép számára biztosítja a védelmet, ám a számítógépek maguk is képesek kell legyenek önmaguk megvédésére – különösen a bástyagép, amelyen nyilvánosan elérhető szolgáltatásokat (ftp, www) futtatunk. Tegyük fel például, hogy nyilvános webkiszolgálódon 2.4-es Linux fut. A gépen helyi Netfilter-szabályok segítségével külön védelmi réteget kell emelni arra az esetre, ha egy támadó megtörné a vállalati tűzfalat, vagy egyéb módon jutna keresztül rajta. Ha a kiszolgálón 2.4-esnél korábbi rendszermag fut, akkor a Netfilter/IP Tables helyett IP Chainst kell használni. Ebben az esetben külső fejlesztőktől szerezhetsz IP Tables-IP Chains fordítómodult, és ennek segítségével használhatod a Firewall Buildert a parancsfájlok elkészítésére.

Visszacsatoló szabályok

Minden tűzfal beállításakor az első lépés – így a bástyagép esetében is – az, hogy teljhatalmat adunk a helyi visszacsatoló felületnek. A visszacsatolóra számos, a helyi folyamatok és démonok között zajló átvitel során van szükség. A helyi hurkot engedélyező szabályok hiányában az IP Tables parancsfájl futtatásakor olyan szolgáltatások szakadnak meg, mint a névszolgáltatás gyorstárazása vagy az SSH-kaputovábbítás.



1. kép A visszacsatoló felületre vonatkozó szabályok

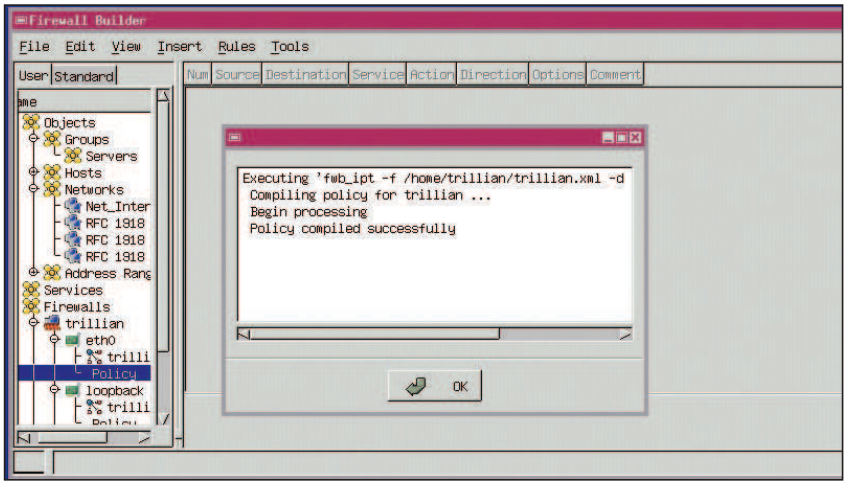


2. kép A bástyagép házirendje

Tegyük fel, hogy van egy Trillian nevű webkiszolgálód, ezt szeretnéd védeni. A Firewall Buildert feltelepítetted rendszergazdai munkaállomásodra – gondolom, még nem felejtetted el, hogy az X Window System, illetve az X alapú alkalmazások nem a bástyagépre valók. Létrehoztad azokat az objektumokat, amelyek a környezetedben lévő állomások, hálózatok és csoportok leírására alkalmasak, továbbá egy Trillian tűzfalobjektumot, majd mindezt egy helyi visszacsatoló felülettel egészítetted ki. Másként fogalmazva: elvégezted a múlt alkalommal ismertetett tennivalókat.

A Trillian helyi visszacsatoló felületéhez két szabályra lesz szükség: az egyik a kimenő, a másik a bejövő forgalmat engedélyezi rajta. A két szabály létrehozásához a következő lépéseket kell követned (*1. kép*):

1. A tűzfal visszacsatoló felületének alobjektuma alatt jobbra, a Firewall Builder ablakának bal oldali részén (az 1. képen loopback névvel szerepel) válaszd ki a visszacsatoló felület házirendjét – egyelőre üresnek kell lennie.



3. kép A házirend lefordítása

2. Kattints a ***Rules*** (Szabályok) menü ***Append rule*** (Szabály hozzáfűzése) pontjára, ekkor az ablak jobb oldali részében egy üres szabály jelenik meg.
3. Húzd a Trillian név melletti tűzfalikont az üres szabály ***Source*** (Forrás) mezőjébe. Ügyelj arra, hogy a kurzornak pluszjellé (+) kell változnia, mielőtt az egérgombot felengednéd.
4. Kattints az egér jobb oldali gombjával az új szabály ***Action*** (Művelet) mezőjébe, majd a menüből válaszd az ***Accept*** (Elfogadás) pontot.
5. Kattints az egér jobb oldali gombjával a szabály ***Direction*** (Irány) mezőjébe, majd válaszd az ***Outbound*** (Kimenő) pontot.
6. Kattints az egér jobb oldali gombjával a szabály ***Options*** (Beállítások) mezőjében található papír- és ceruzaikonra, majd válaszd a Turn logging ***OFF*** (Naplózás kikapcsolása) beállítást.
7. A jobb oldali egérgombbal kattints újra a szabály ***Options*** mezőjébe, majd válaszd a ***Modify options*** (Beállítások módosítása) parancsot. A megnyíló ablakban jelöld be az alul található jelölőnégyzetet, ezzel kikapcsolod az állapotalapú vizsgálatot. Semmi szükség arra, hogy a processzor erőforrásait a helyi hurkon keresztül folyó forgalom állapotalapú követésére pocsékoljuk.
8. Ha gondolod, az egér jobb oldali gombjával kattints az új szabály ***Comment*** (Megjegyzés) mezőjébe, válaszd az ***Edit Comment*** (Megjegyzés szerkesztése) parancsot, és készíts rövid feljegyzést a szabály szerepéről, céljáról (például „Helyi visszacsatoló felületkimenet engedélyezése”).

Az 1. képen is látható második szabály létrehozásához ismételd meg a 2–8. számú lépést. A 3. lépésben a Trillian ikonját értelemszerűen az új szabály ***Destination*** (Cél) mezőjébe kell húznod, és nem a forrásba. Az 5. lépésben az irányt ***Inbound*** (Bejövő) értékre állítsd.
Jogos a kérdés: pontosan hogyan működnek ezek a szabályok? Először is hangsúlyoznom kell, hogy kizárólag a helyi visszacsatoló felületre vonatkoznak. Bármelyik felületnek lehetnek saját szabályai, ezek feldolgozása a tűzfal általános szabályainak érvényre juttatása előtt történik meg. Bár ennél a két visszacsatoló szabálynál a Trillian cél és forrás is volt egyben, szó sincs arról, hogy e két szabály a Trillian bármelyik IP-címére is érvényes lenne. Kizárólag a helyi visszacsatoló felületen kimenő és beérkező csomagokra vonatkoznak.
El is érkeztünk a visszacsatoló szabályokkal kapcsolatos utolsó tudnivalóhoz. Feleslegesnek tűnhet két olyan szabályt létrehozni, amelyek ugyanúgy a tűzfalra vonatkoznak, és nem egyetlen, bármely forrást és bármely célt elfogadó szabályba sűríteni őket. Jómagam azonban úgy tapasztaltam, hogy amikor egyetlen szabályt hoztam létre, a Firewall Builder az `INPUT` és az `OUTPUT` helyett a `FORWARD` láncba írta a visszacsatoló szabályokat, ami viszont a visszacsatoló felület használhatatlanná válását okozta. Ha külön kimeneti és bemeneti szabályt hoztam létre a visszacsatolóhoz, a hiba eltűnt. Aggodalomra nincs ok, tapasztalataim szerint ez az egyetlen olyan helyzet, amikor a Firewall Builder rossz láncba írja a szabályokat. A hiba csak egylaki gépeknél jelentkezett, több felülettel is rendelkező tűzfalaknál nem.

A bástyagép házirendje

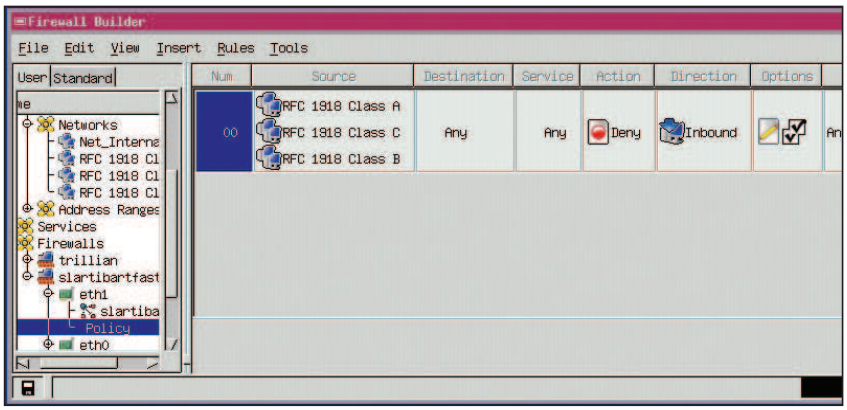
Miután a bástyagép visszacsatoló felületét lerendeztük, fordítsuk figyelmünket az általános házirendre. Ehhez némi tervezésre is szükség lesz. A cél nyilván az, hogy a Netfilter megfelelő védelmet nyújtson, de eközben a használhatóságot se korlátozza. Példagépünk, a Trillian egy webkiszolgáló, a többi állomás tehát HTTP és HTTPS protokollon keresztül fogja elérni. A megfelelő naplózás érdekében szeretnénk, ha a Trillian DNS-lekérdezéseket is végre tudna hajtani. Emellett bizonyos felügyeleti jellegű kapcsolatokra is szükség lehet. Erre a célra SSH-t fogunk használni, tehát a bejövő SSH-kapcsolatokat is engedélyeznünk kell, de csak a belső hálózat felől. A *2. képen* egy ilyen, a Trillian számára készített házirendet láthatunk.
Az egyes szabályok létrehozásának aprólékos ismertetésétől most eltekintenék, néhány dologra viszont érdemes kitérni. Először is az ablak bal oldalán megjelenő objektumfában látható, hogy közvetlenül a Trillian alatti ágban választottam ki az általános ***Policy*** (Házirend) objektumot, és nem a felületekre külön vonatkozó házirendobjektumok között. Nemcsak a Trillian objektumot használtam fel, hanem egy ***Net_Internal*** nevű hálózatobjektumot is, ami a múltkori írásom egyik példaobjektuma. Ez egy teljes hálózatnyi IP-címtartományra hivatkozik, pontosabban a 192.168.111.0 hálózatra. Míg a második szabály forrásként egyetlen IP-címet jelöl meg (a Trillian IP-címét), addig a harmadik szabály mindazokra a csomagokra érvényes, amelyeknek a forrás IP-címe a 192.168.111.1 – 192.168.111.254 tartományba esik.
Egy másik fontos tanács a szabályok létrehozásával kapcsolatban: bátran használd fel a Firewall Builder beépített szolgáltatásobjektumait, amelyeket a bal oldali ablakrész ***Standard*** fülére kattintva érhetsz el. Némi figyelem természetesen nem árt, mert ha a szolgáltatásobjektumok (például `dns_tcp`) szabályokba való húzogatásától eltérő műveletet is végzel, akkor az ablak jobb oldalán látható szabályok helyett az éppen kiválasztott elem tulajdonságai jelennek meg.
Egy kicsit pontosítva, ha éppen egy házirendet állítasz össze, akkor a ***Standard*** fülre, majd az objektumfa + (lenyitás) és – (összezárás) ikonjaira kattintva, illetve a szolgáltatásobjektumokat a megfelelő helyre húzva kényelmesen dolgozhatsz, a jobb oldali ablakrész által

A trillian.fw fájl tartalma

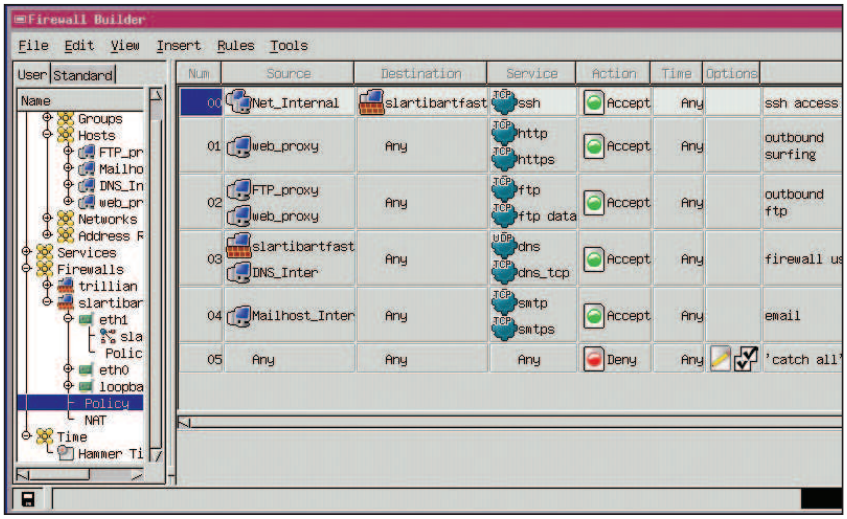
```
#!/bin/sh
#
#  Firewall Builder  fwb_ipt v1.0.8-3
#
#  Generated Tue Mar 11 08:01:21 2003 CST

log() {   if test -x "$LOGGER"; then
    logger -p info "$1"
  fi
}

MODPROBE="/sbin/modprobe"
IPTABLES="/sbin/iptables"
IP="/sbin/ip"
LOGGER="/usr/bin/logger"

cd /etc || exit 1

log "Tűzfalparancsfájl indítása…"

va_num=1

FWD=´cat /proc/sys/net/ipv4/ip_forward´
echo "0" > /proc/sys/net/ipv4/ip_forward
echo 30 > /proc/sys/net/ipv4/tcp_fin_timeout
echo 1800
➥> /proc/sys/net/ipv4/tcp_keepalive_intvl

$IP -4 neigh flush dev eth0
$IP -4 addr flush dev eth0 label "eth0:FWB*"

$IPTABLES -P OUTPUT  DROP
$IPTABLES -P INPUT   DROP
$IPTABLES -P FORWARD DROP

cat /proc/net/ip_tables_names | while read
     ➥table; do
  $IPTABLES -t $table -L -n |   while read c
              ➥chain rest; do
      if test "X$c" = "XChain" ; then
        $IPTABLES -t $table -F $chain
      fi
  done
  $IPTABLES -t $table -X
done

$IPTABLES -A INPUT   -m state --state
➥ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT  -m state --state
➥ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A FORWARD -m state --state
➥ESTABLISHED,RELATED -j ACCEPT

# Rule 0(lo):  Outbound from loopback
$IPTABLES -A OUTPUT  -o lo -j ACCEPT

# Rule 1(lo): Inbound from loopback
$IPTABLES -A INPUT  -i lo -j ACCEPT

# Rule 0(global)
$IPTABLES -A INPUT -p tcp  -m multiport
➥--destination-port 80,443  -m state
➥--state NEW -j ACCEPT

# Rule 1(global)
$IPTABLES -A OUTPUT -p tcp  --destination-
➥port 53 -m state --state NEW -j ACCEPT
$IPTABLES -A OUTPUT -p udp  --destination-
➥port 53 -m state --state NEW -j ACCEPT

# Rule 2(global)
$IPTABLES -A INPUT -p tcp  -s
➥192.168.111.0/24  --destination-port 22
➥-m state --state NEW -j ACCEPT

# Rule 3(global)
$IPTABLES -N RULE_3
$IPTABLES -A FORWARD -j RULE_3
$IPTABLES -A RULE_3 -j LOG  --log-level
➥warning --log-prefix "RULE 3 -- DROP "
➥--log-ip-options
$IPTABLES -A RULE_3 -j DROP

echo 0 > /proc/sys/net/ipv4/ip_forward
```

megjelenített adatok köre nem változik meg. Ha viszont egyszerűen kiválasztasz egy szolgáltatásobjektumot vagy -kategóriát a ***Standard*** fában (olyan módon, hogy rákattintasz, de nem húzod át sehova), akkor ennek az objektumnak a tulajdonságai jelennek meg a jobb oldalon. Ilyenkor vissza kell lépned a ***User*** (Felhasználó) lapra, újra ki kell választanod a tűzfal általános házirendjét, és csak ekkor jelennek meg újra a szabályok. Adatvesztés nem történik, de kényelmetlen és bosszantó jelenség. Sokkal fontosabb, hogy ezeknél a szabályoknál az állapotalapú vizsgálatot bekapcsolva hagytam, vagyis kihagytam a visszacsatoló szabályok kapcsán ismertetett eljárás 7. lépését. Normál esetben szeretnénk, ha a rendszermag megőrizné a hálózati átvitelekkel kapcsolatos állapotadatokat – éppen ez az, aminek köszönhetően a legtöbb átvitel egyetlen kétirányú szabállyal leírható, és nincs szükség két-két egyirányú szabályra. Az állapotalapú vizsgálatnak köszönhető például az, hogy ha egy átvitel megfelel a *2. képen* látható 2. szabály előírásának, ami engedélyezi a bejövő SSH-forgalmat a belső hálózat gépeiről, akkor a Trillian rendszermagja nemcsak a bejövő SSH-csomagokat engedélyezi, de a Trillian által válaszként küldötteket is. Ha a második szabálynál kikapcsoltam volna az állapotalapú vizsgálatot, akkor a Trillian 22-es TCP-kapujáról származó csomagok továbbításának engedélyezésére, és ezzel a válaszok elküldésének lehetővé tételére egy másik szabályt is létre kellett volna hoznom.

Végül az utolsó kivételével mindegyik szabály esetében ki kell kapcsolni a naplózást, a fenti eljárás 6. lépésében leírt módon. Sokan úgy gondolják, nincs értelme és haszna lemezhelyet és be-, illetve kiviteli terhelést áldozni arra, hogy a rendszer a tűzfalszabályok által feldolgozott csomagok mindegyikét



4. kép A házirend lefordítása



5. kép Általános házirend egy tűzfalhoz

naplózza. Valóban, én is inkább az eldobott csomagokat naplózom, az engedélyező szabályok naplózásától pedig eltekintek. A 2. képen látható mintaszabályok sora egy általános szabállyal zárul: ez az összes olyan csomagot eldobja, amelyik sem az előtte található szabályok valamelyikének, sem a felületekre külön megadott szabályoknak – például a helyi visszacsatolóra vonatkozó házirendnek – nem felel meg.
Ennek a szabálynak tulajdonképpen kizárólag a naplózásban van szerepe.
A Firewall Builder az alapértelmezett házirendet az összes IP Tables lánc esetében `DROP`-ra állítja, de ezeket az alapértelmezés szerint eldobott csomagokat a rendszer nem naplózza, hacsak a Netfiltert nem utasítjuk kifejezetten erre. Létezik már kísérleti jellegű folt a Netfilterhez, ami alapbeállítás szerint is lehetővé teszi az összes eldobott csomag naplózását, de szerintem érdemes megvárni a kód üzembiztossá válását, és csak azután fordítanám bele a rendszermagba. Ha ezt valamiért nem akarod megvárni, akkor ezt a szolgáltatást úgy érheted el, hogy a Firewall Builderben kiválasztod a tűzfalobjektumot, rákattintasz a hozzá tartozó ***Firewall Properties*** (Tűzfal tulajdonságai) fülre, majd bejelölöd a ***Log all dropped packets*** (Naplózzon minden eldobott csomagot) jelölőnégyzetet. Az említett foltról a ➲ http://www.netfilter.org/documentation/pomlist/pom-summary.html címen találhatsz további tájékoztatást.

A házirend lefordítása és telepítése

Miután a tűzfal házirendje elkészült, IP Tables-parancsfájllá kell alakítani. Ehhez először ellenőrizni kell, hogy az ablak bal oldali részén megjelenő fában a tűzfal objektuma és az általános házirend vagy a felületekhez rendelt saját házirendek valamelyike ki van-e választva. Ezt követően nyisd meg a ***Rules*** (Szabályok) menüt, és válaszd a ***Compile*** (Fordítás) pontját. Az eredmény a *3. képen* látható. A házirend sikeres lefordítása után a Firewall Builder egy fájlba írja az eredményt, aminek a neve annak a tűzfalnak a nevével egyezik meg, amelyhez a lefordított házirend tartozik, a kiterjesztése pedig *.fw*. A létrejött példaparancsfájl, a ***trillian.fw*** tartalma – a terjedelem miatt kissé módosítva, rövidítve – a *listában* látható. Az írásomban említett szabályok mindegyike megtalálható benne.
Az új parancsfájlt kézzel is átmásolhatod a Trillianre, majd változatlan formában futtathatod, vagy kézzel is lefordíthatod egy olyan indítási parancsfájlba, amely a Trillian Linux-terjesztésének megfelel, például egy szabványos Red Hat 7.3 indítási parancsfájlba. Könnyebb önműködő módon átmásolni és üzembe helyezni egy a Firewall Builderhez készült telepítő parancsfájl segítségével. Ilyenre példa az `fwb_install`, amely a ➲ http://sourceforge.net/project/showfiles.php?group_id=5314 címről érhető el. Utóbbi különösen elegáns és egyszerű módja a tűzfalszabályok biztonságos átmásolásának és üzembe helyezésének, az `fwb_install` ugyanis `scp`-n keresztül másolja a parancsfájlt a távoli gép */etc/firewall* könyvtárába, majd SSH-n keresztül indítja el. Ha az `fwb_install`-t már valahová letöltötted a Firewall Buildert futtató gépeden, akkor a Firewall Builderen belül az egyes tűzfalobjektumok ***Compile***/***Install*** (Fordítás/Telepítés) tulajdonságai között írhatod elő a használatát. Ne feledd az `fwb_install`-t a rendszered beállításainak megfelelően módosítani, illetve az általa használandó SSH-kulcsokról is gondoskodnod kell. Miután ezekkel végeztél, a szabályok lefordítás utáni telepítéséhez mindössze a ***Rules*** (Szabályok) menü ***Install*** (Telepítés) pontjára kell kattintanod.
Az `fwb_install` ügyes segítőtárs, ám szükséged lesz egy olyan indítási parancsfájlra is a célrendszeren, amelyik indításkor mindig futtatja a tűzfalparancsfájlt. Egyébként a rendszer védtelen lesz minden indítás vagy újraindítás és a között az időpont között, amikor a Firewall Builder `Install` parancsát lefuttatod. A saját rendszered */etc/init.d* könyvtárában található fájlok megfelelő mintául szolgálnak ehhez.

Házirend egy valódi tűzfalhoz

Írásom jelentős részét a bástyagépes példának szenteltem, ám szerencsére egy többlaki (több felülettel is rendelkező) tűzfal házirendjét is nagyon hasonló módon lehet összeállítani. A visszacsatoló szabályokkal kell kezdeni, a többi felületen meg kell akadályozni a hamisításokat, létre kell hozni egy általános házirendet, lefordítani és végül telepíteni. A legfontosabb különbség az, hogy egy

tűzfal – a kiszolgálók többségével ellentétben – több hálózati felülettel is rendelkezik. Mivel egy egyetlen felülettel rendelkező rendszer a visszacsatolótól eltekintve az összes csomagot ugyanazon a fizikai eszközön keresztül kapja, a hamisított csomagokat nem tudja megkülönböztetni a valódiaktól, és minden csomag forrás-IP-címét kénytelen elfogadni. Egy többlaki rendszer ezzel szemben könnyedén szét tudja válogatni azokat a csomagokat, amelyek ténylegesen a helyi hálózatról érkeznek, illetve azokat, amelyek valójában az Internet felől futottak be, de olyan hamis forrás IP-címmel, ami helyi vagy megbízható hálózatból jövőnek láttatja őket.

Példámban a belső hálózat a 192.168.111.0 (alhálózati maszk: 255.255.255.0) címet kapta. Ha van egy Slartibartfast nevű tűzfal, amely e hálózat és a külvilág között helyezkedik el, akkor hamisításellenes szabályokkal utasíthatjuk arra, hogy a belső hálózat felé vezetőtől eltérő felületeken azonnal dobjon el minden olyan csomagot, amelynek forrás IP-címe 192.168.111-gyel kezdődik. Az ilyen csomagok nyilvánvalóan hamisak.

A *4. képen* a Slartibartfast hamisításellenes szabálya látható.

Mielőtt ezt a szabályt létrehoztam volna, olyan hálózatobjektumokat készítettem, amelyek a 1918-as RFC-ben („Address Allocation for Private Internets”) foglalt, fenntartott IP-címtartományokat fedik le. Az RFC 1918 címtartományai kizárólag szervezeteken belüli használatra valók, az Interneten keresztül nem irányíthatók, így minden internetes tűzfalnak eleve feltételeznie kell, hogy az ilyen forráscímmel érkező csomagok hamisak – a 4. képen látható szabály pontosan erről gondoskodik. Mivel nálam az RFC 1918 szerinti C osztályú objektum a 192.168.0.0 tartományba esik (alhálózati maszk: 255.255.0.0), belsőhálózati címem pedig 192.168.111.0 (része az RFC 1918 által megadott címtérnek), a `Net_Internal` objektumot ebben a szabályban nem kellett szerepeltetnem. Egyébként, ha valaki nem ismerné a 1918-as RFC tartalmát, az RFC 1918 A osztályú objektumom a 10.0.0.0 címre (alhálózati maszk: 255.0.0.0), az RFC 1918 B osztályú pedig a 172.16.0.0 címre (alhálózati maszk: 255.240.0.0) hivatkozik.

Általános szabályok

Az *5. képen* a Slartibartfast általános házirendje látható, ennek részletes ismertetését mellőzném – mondandóm már így is túl hosszúra nyúlt. Mivel a Firewall Builder lényege éppen a tűzfalszabályok könnyen olvasható formában való megjelenítése, az 5. kép értelmezése talán nem okoz különösebb gondot.

Ha már a könnyű megértésről esik szó: talán még nem említettem, hogy a helyi visszacsatolóra vonatkozó, hamisításellenes és általános szabályok egyaránt könnyedén létrehozhatók a Firewall Builder szabályvarázslójával.

Remélem, bocsánatos bűn a részemről, hogy csak most említem a varázslót. A tűzfalszabályok azonban túl fontosak ahhoz, hogy elkészítésükkor holmi varázslóban vakon megbízzunk.

Linux Journal 2003. június, 110. szám

Mick Bauer (mick@visi.com) Biztonsági szakember, a Linux Journal biztonsági témákkal foglalkozó szerkesztője, biztonsági tanácsadó a Minnesota állambeli Minneapolisban található Upstream Solutions LLC Inc.-nél. Mick szabadidejében a gyermekeivel fogócskázik vagy zenél – néha mindkettőt egyszerre.