Slovenská technická univerzita v Bratislave
Fakulta elektrotechniky a informatiky

Firewally

Príprava na prezentáciu na predmet Počítačové siete 2

autor: Róbert Trebula
rok: 2001

Obsah

1 Čo je firewall

1.1 Definícia

Firewall je zariadenie, alebo skupina zariadení určená na implementáciu a presadenie časti bezpečnostnej politiky organizácie. Ide o **zabezpečenie komponentov počítačovej siete** (počítačov, serverov, úložných dátových zariadení a pod.) a používateľských informácií na nich uložených pred potenciálnymi útokmi a inými bezpečnostnými hrozbami.

Umožňuje definovať pravidlá pre sieťovú komunikáciu na rôznych úrovniach a tak presadiť použitú bezpečnostnú politiku organizácie v oblasti komunikácie na počítačovej sieti.

1.2 Činnosť firewallu

Základným princípom činnosti sieťového firewallu je **blokovať alebo prepúšťať sieťovú komunikáciu medzi sieťami**. Rozhodnutie, či danú komunikáciu umožní alebo nie sa odvíja od nastavenej politiky.

Popri hlavnej činnosti – riadenia sieťovej prevádzky, plní firewall aj niekoľko ďalších, viac či menej užitočných funkcií:

- Monitorovanie a zaznamenávanie bežnej (povolenej) sieťovej prevádzky. Takto získané údaje môžu byť cenným zdrojom informácií pre manažment organizácie o efektívnosti využívania prvkov sieťovej konfigurácie jednotlivými používateľmi.
- Monitorovanie a zaznamenávanie pokusov o porušenie bezpečnostných pravidiel na sieti. Takéto pokusy môžu byť vedené buď zo strany internetu na privátnu sieť, z privátnej siete na internet, alebo medzi uzlami privátnej siete. Firewall môže veľmi účinne monitorovať a brániť prvým dvom typom porušenia pravidiel, kým porušenie v rámci siete nemá možnosť priamo ovplyvniť a mnohokrát ani zistiť.
- Podpora prevádzky sieťových aplikácií a protokolov. Ak funguje firewall ako gateway (na aplikačnej vrstve), môže efektívne podporovať dotyčné protokoly (napr. ak slúži ako http-proxy server, môže znižovať prevádzku medzi našou sieťou a internetom tým, že bafruje niektoré údaje - cache).
- Poskytovanie služby verejného vstupného bodu privátnej siete. Firewall môže slúžiť zároveň ako web server, mejlový server a podobne. Takto bude spájať nielen privátnu sieť s internetom, ale aj internet s privátnou sieťou, pravda len v medziach určených požiadavkami organizácie.

1.3 Pred čím firewall vnútornú sieť nechráni

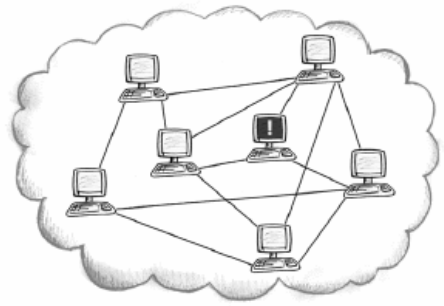
Zjednodušene povedané – **firewall nechráni pred prevádzkou, ktorá ním neprechádza**.

Dáta totiž do a z organizácie môžu prúdiť rôznymi cestami. Okrem komunikácie s internetom cez firewall do organizácie prichádzajú zamestnanci, nosia si domov údaje na disketách. Pripájajú sa na internet cez modemy. Komunikujú cez telefóny a podobne.

Jedným zo zdrojov potenciálneho nebezpečenstva je nerozumné nebezbečné správanie sa používateľov vo vnútornej sieti.

Firewall poskytuje len ,,perimetrickú ochranu" – chráni len dve siete od seba navzájom, nechráni jednotlivé uzly jednej podsiete (bezpečnostnej domény) od útokov z tej istej podsiete.

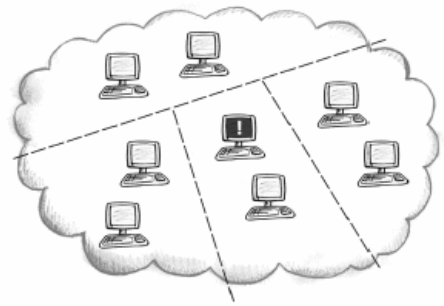
Ak sa útočníkovi (z vonku alebo z vnútra privátnej siete) podarí získať kontrolu nad jedným uzlom siete, môže tým pádom využiť všetky možnosti, ktoré majú legálni používatelia siete (obrázok 1). Takto môže závažným spôsobom narušiť bezpečnosť celej



Obrázok 1: Hrozba útoku na celú privátnu sieť z jedného získaného uzla

podsiete – bezpečnostnej domény.

Riešením takejto hrozby je rozdeliť privátnu sieť na niekoľko bezpečnostných domén (obrázok 2). Takto získa útočník možnosť využívať výhody vnútornej siete len v rámci jed-



Obrázok 2: Útok z jedného uzla sa obmedzí v rámci jednej bezpečnostnej domény

nej bezpečnostnej domény, Na oddelenie jednotlivých bezpečnostných domén je výhodné použiť firewall.

Rovnako ako je nezmyselné mať pancierové dvere s niekoľkými bezpečnostnými zámkami na drevenom domčeku, je nezmyselné inštalovať firewall do prostredia so žiadnou alebo slabou bezpečnostnou politikou. Preto musí byť sieťový firewall jej neoddeliteľnou súčasťou.

Ďalej firewall nechráni pred ,,tunelovaním" vyšších protokolov. Firewall nemôže zabrániť, aby obsahom dát prechádzjúcich cez povolené protokoly neboli dáta, ktoré by firewall neprepustil. Ako príklad sa dá uviesť napríklad tunelovanie telnetu cez http.

1.4 Oblasti použitia

Firewall slúži na oddelenie sietí. Môže ísť o jeden alebo kombináciu nasledovných dôvodov:

- oddelenie vnútornej siete od internetu
- oddelenie častí privátnej siete s rôznym stupňom zabezpečenia
- oddelenie častí privátnej siete s rôznym stupňom dôvery
- oddelenie častí privátnej siete z dôvodov zmenšenia dopadu prípadného vnikuntia a zneužitia

2 Prečo inštalovať firewally

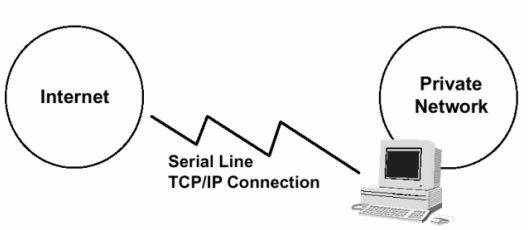
Internet nie je práve najbezpečnejším miestom, kde by sa mohla organizácia ocitnúť. Jeho veľkosť, anonymita a nízka úroveň zabezpečenia ho robí lákavým miestom pre ľudí, ktorí majú úmysly a schopnosti poškodiť organizáciu z rôznych dôvodov.

Keď chce organizácia na internete pracovať bez toho, aby jej činnosť mohla byť kedykoľvek paralyzovaná útokom z vonku, aby sa dôverné informácie jej a jej partnerov, zamestnancov nedostali do nepovolaných rúk a aby nedošlo k poškodeniu jej majetku, funkčnosti, povesti či celkovej konkurencieschopnosti, je dôležité **zakomponovať sieťovú bezbečnosť do celkovej bezpečnostnej politiky** organizácie.

Firewall je dôležitým prvkom implementácie bezpečnostnej politiky, pretože umožňuje efektívne presadzovať túto politiku v oblasti komunikácie medzi privátnou sieťou a internetom a medzi podsieťami privátnej siete.

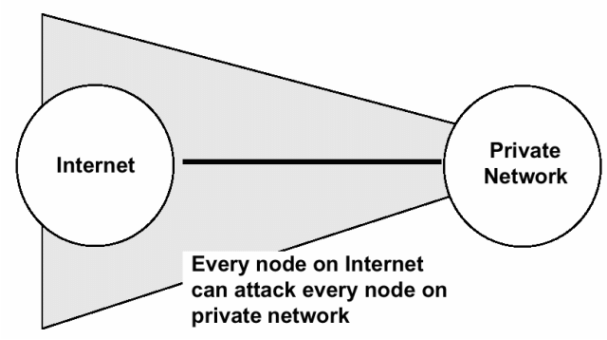
V ďalších dvoch častiach ukážeme rozdiel medzi sieťou bez firewallu (teda s priamym spojením na internet) a sieťou pripojenou na internet cez firewall. Ako dôležitý pojem sa zavádza tzv. **riziková zóna**. Je to podmnožina objektov bezpečnostnej politiky (v tomto prípade privátnej siete), ktorá je vystavená priamym hrozbám z prostredia.

2.1 Privátna sieť pripojená na internet bez firewallu



Obrázok 3: Spojenie privátnej siete s internetom bez firewallu

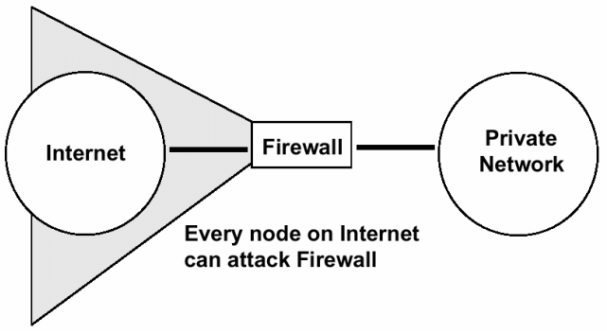
Obrázok číslo 3 znázoňuje pripojenie privátnej siete na internet bez firewallu. Rizikovou zonou je v takomto prípade celá vnútorná sieť ako ukazuje obrázok 4.



Obrázok 4: Riziková zóna privátnej siete bez firewallu

2.2 Spojenie privátnej siete s internetom cez firewall

Obrázok 5 znázorňuje fakt, že pri spojení privátnej siete s internetom cez firewall je rizikovou zónou len firewall[1]. Preto je tento nutné zabezpečiť tak, ako by v pred-



Obrázok 5: Riziková zóna privátnej siete s firewallom

chádzajúcom prípade museli byť zabezpečené všetky uzly privátnej siete. Už len náklady na zabezpečenie všetkých uzlov privátnej siete na takú úroveň odolnosti voči sieťovým útokom sú v drvivej väčšine prípadov väčšie ako náklady na firewall. A to sme ešte vôbec nebrali do úvahy ostatné prínosy firewallu pre organizáciu.

Ako vyplýva z predchádzajúcej úvahy, vytvorenie firewallu má pozitívny ekonomický dopad na organizáciu, najmä z dlhodobého hľadiska s ohľadom na prevenciu voči možným stratám vyplývajúcich z narušenia bezpečnosti organizácie cez počítačovú sieť.

3 Návrh firewallu

3.1 Kľúčové aspekty návrhu firewallu

Základnými otázkami pri návrhu firewallu sú najmä otázky celkovej bezpečnostnej politiky organizácie. Ide o zvolenie paradigmy bezpečnosti, miery monitorovania, redundancie

[1] Tento obrázok je samozrejme len ilustratívny a nemusí platiť pre akúkoľvek konfiguráciu s firewallom, viď časť 5

a riadenia, finančné otázky. Technické aspekty by mali vyplynúť z predchádzajúcich aspektov a nie naopak.

3.2 Základné paradigmy riadenia premávky

V podstate sú možné dva prístupy k riadeniu prevádzky cez firewall:

- čo nie je povolené, je zakázané
- čo nie je zakázané, je povolené

Pri prvom prístupe sa identifikujú služby, ktoré sú pre fungovanie organizácie nevyhnutné, poskytujú primeranú úroveň bezpečnosti a sú dobre vyskúšané a zdokumentované. Všetky ostatné služby, protokoly, aplikácie sa zakážu a firewall ich dáta nebude prenášať medzi sieťami. Táto paradigma je považovaná za konzervatívnejšiu, vychádza z princípu ,,čo nepoznám mi môže ublížiť" Jej implementácie sú ľahšie monitorovateľné a ovládateľné, avšak môže viesť k prílišnému obmedzovaniu.

Pri druhom prístupe sa identifikujú služby, ktoré predstavujú bezpečnostné riziká a tieto sa zakážu, prípadne nahradia bezpečnejšími. Tento prístup je flexibilnejší a vedie k menej obmedzujúcim riešeniam, avšak sú tu riziká zneužitia používateľmi (napríklad keď je zakázaný na firewalle port 23 na telnet z vonku, nejaký používateľ si môže telnet presunúť na iný port, ktorý nie je zakázaný a tým vniesť za firewall zakázaný protokol).

Ak máme vysoký stupeň dôvery v používateľov vo vnútornej sieti, môžeme s výhodou využiť prístup: z vonku zakázať všetko, čo nie je povolené a z vnútra povoliť všetko, čo nie je zakázané.

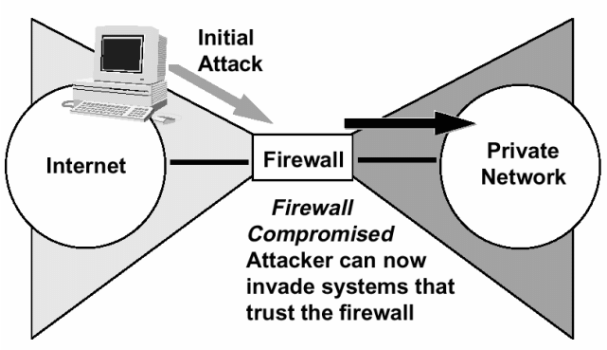
Ak je jednou z úloh firewallu aj chrániť internet pred používateľmi privátnej siete, je potrebné zvoliť z oboch strán ,,paranoický" prístup.

3.3 Analýza rizík

Analýza rizík spočíva v hľadaní odpovedí na otázky typu:

- koľko je potenciálnych možností na útok na firewall?
- ako by útok pokračoval, keby sa mu podarilo prekonať prvú prekážku?
- v akom bode sa stane útok nevystopovateľný?
- v akom bode je zrútený celý bezpečnostný systém?
- aké musia byť opatrenia v prípade, že nastane útok?

Je dôležité aj analyzovať, čo sa stane, keď bude prekonaný samotný firewall (obr. 6). V takomto prípade sa stane rizikovou doménou celá privátna sieť. Je potrebné určiť presný postup činnosti v takomto prípade.



Obrázok 6: Riziková zóna po prekonaní firewallu

4 Delenie firewallov

4.1 Delenie podľa vrstvy OSI modelu

4.1.1 Filtrovanie paketov

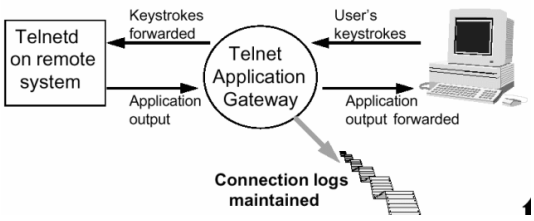
Ak prebieha filtrovanie prevádzky na sieťovej vrstve, hovoríme o **firewalloch s filtrovaním paketov**. V tomto prípade sa monitorujú jednotlivé prichádzjúce a odchádzajúce pakety. Podľa definovaných pravidiel sa kontrolujú ich hlavičky a rozhoduje sa, čo sa s nimi urobí. Ak spĺňajú podmienky, budú prepustené na druhú stranu firewallu. Ak nie, môžu byť zahodené, prípadne sa ich výskyt zaznamená ako pokus o porušenie pravidiel.

Pre aplikácie je takýto firewall transparentný – nevidia ho. Môžu vytvárať spojenie priamo na požadovaný uzol na opačnej strane firewallu bez toho, aby vedeli, že táto komunikácia ide cez firewall.

Paketové filtre sa implementujú hardvérovo, alebo softvérovo. V druhom prípade bežia na počítači, ktorý vystupuje ako firewall a to zväčša v móde jadra. V oboch prípadoch sú pomerne rýchle a s výhodou sa zabudujú priamo do smerovačov medzi dvomi sieťami.

4.1.2 Proxy servery

Ak prebieha filtrovanie prevádzky na aplikačnej vrstve, hovoríme o **aplikačných proxy serveroch**. Proxy server tvorí medzičlen medzi klientom, ktorý požaduje nejakú službu a serverom, ktorý mu ju poskytuje.



Obrázok 7: Proxy server

Pre aplikácie takýto firewall nie je transparentný – pre jeho použitie ich treba prekonfigurovať. Aplikácia sa pripojí na proxy server, zadá mu svoju požiadavku a tento sa rozhodne, či ju splní alebo nie. Ak sa rozhodne ju splniť, pripojí sa na server v druhej sieti a predá výsledok aplikácii.

Aplikačné proxy servery sa implementujú ako procesy na počítači, ktorý má prístup na obe siete. Sú síce pomalšie ako paketové filtre, ale pretože rozumejú protokolu, ktorý spracovávajú, umožňujú lepšie možnosti nastavovania kontroly pre daná aplikačné protokoly ako paketové filtre. Ich ďalšou výhodou je, že môžu slúžiť aj ako bafer požiadaviek. Najčastejšie sa používajú proxy servery pre protokoly http, ftp.

4.2 Stavové a bezstavové firewally

Toto delenie sa týka najmä paketových filtrov, ale v niektorých prípadoch by sa dalo aplikovať aj na proxy servery.

4.2.1 Bezstavové filtre

Bezstavové firewally kontrolujú každý paket nezávisle na ostatných. Ich implementácia je jednoduchšia (nevyžadujú pamäť), avšak v niektorých prípadoch sa ťažšie konfigurujú.

4.2.2 Stavové filtre

Stavové filtre si udržiavajú informácie o jednotlivých spojeniach. Tieto informácie potom používajú na určenie osudu týchto, ale aj nasledujúcich spojení.

Ich prevádzka si vyžaduje väčšie pamäťové nároky, ale konfigurovanie a funkčnosť takýchto filtrov je najmä s ohľadom na vyššie protokoly lepšia.

4.3 Delenie podľa poskytovateľa

Jedná sa o rozhodnutie, aký produkt bude nasadený a kým.

4.3.1 Black-box

Výrobca poskytuje inštaláciu, konfiguráciu a podporu svojho produktu. Na druhej strane neposkytuje podrobnú a verifikovateľnú špecifikáciu produktu najmä z bezpečnostného hľadiska („trust us" bezpečnostný model). Takéto riešenia sú v drvivej väčšine prípadov ekonomicky náročné.

4.3.2 Crystal-box

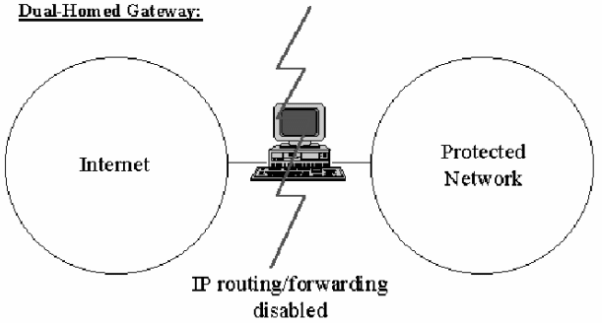
Produkt si inštaluje organizácia sama, alebo si na to najme konzultanta. Zdrojové kódy a dokumentácia je k dispozícii a dá sa analyzovať z hľadiska bezpečnosti. Sú však problémy s kompatibilitou prvkov a jednoduchosťou inštalácie, konfigurácie a správy systému. Takéto riešenie, najmä na báze open-source produktov je z ekonomického hľadiska lacnejšie.

5 Konfigurácie s firewallmi

Je možných niekoľko rôznych typov konfigurácií spojenie dvoch sietí cez firewall. Vo väčšine z nich vystupuje jeden, alebo viacero uzlov pripojených na privátnu sieť, označený ako **bastion host**. Tento počítač je síce súčasťou privátnej siete, ale je prístupný aj z vonkajšej siete. Preto sa naň kladú maximále nároky na odolnosť voči útokom.

5.1 Dual-homed gateway

Táto konfigurácia je založená na uzle s pripojením do oboch sietí. Smerovanie medzi nimi je **zakázané**. Uzly z privátnej siete sa naň môžu pripájať, rovnako aj uzly z vonkajšej



Obrázok 8: Konfigurácia dual-homed gateway

siete. Priama komunikácia medzi uzlami privátnej a vonkajšej siete je však zakázaná. Tento počítač je využitý ako základňa pre rôzne aplikačné proxy servery, alebo paketové filtre.

Ak majú na tento počítač prístup používatelia internej siete (napr. ak chcú posielať mejly a nebeží to SMTP proxy), musí byť ich správanie kontrolované, pretože by mohli vážne narušiť bezpečnosť. Vo všeobecnosti sa neodporúča vytvárať na tomto počítači žiadne kontá používateľom.

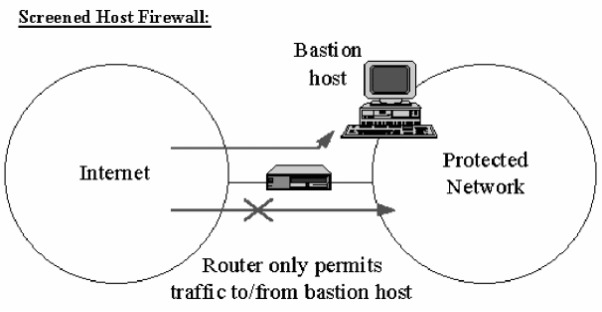
5.2 Screened host

Toto je len variácia konfigurácie s dual-homed gateway-om, kde je spojenie realizované cez smerovač. Smerovač je nastavený tak, že prepúšťa prevádzku z vonkajšej siete len na screened host, nie do vonkajšej siete. Takisto neprepúšťa prevádzku z vnútornej siete priamo na vonkajšiu sieť.

Tento smerovač (nazývaný aj **screening router**) musí byť kvalitný a musí odolať útokom. Môže plniť úlohu paketového filtra – to znamená firewallu s možnosťou vykonávať NAT. Môže aj rozdeľovať sieť na bezpečnostné domény.

Pre zabezpečenie bastion hostu v tejto konfigurácii platia tie isté pravidlá, ako pre dual-homed gateway.

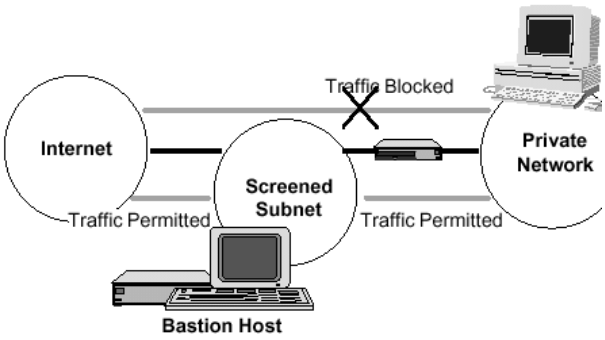
Táto konfigurácia sa pre účely riadenia bezpečnosti sieťovej prevádzky používa najčastejšie, najmä pre svoju flexibilitu.



Obrázok 9: Konfigurácia screened host

5.3 Screened subnet

V tejto konfigurácii vystupuje skupina uzlov nazývaná aj **demilitarizovaná zóna** (DMZ). Na túto je prístup aj z vonkajšej aj z vnútornej siete. Jedná sa o zložitejšiu



Obrázok 10: Konfigurácia screened subnet

architektúru, ktorá delí privátnu sieť an dve časti – demilitarizovanú zónu a privátnu zónu.

V demilitarizovanej zóne sú umiestnené napr. web servery, mejlové servery a podobne. Tieto sú priamo prístupné z vonkajšej siete a môžu jej poskytovať služby.

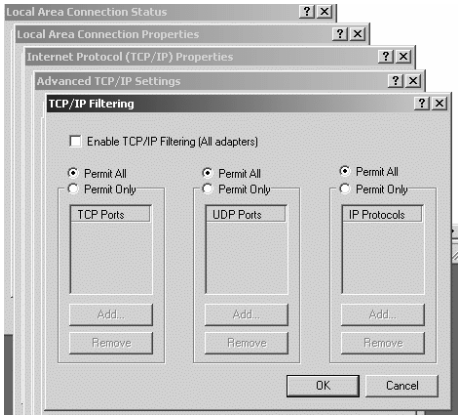
Uzly privátnej siete sú neviditeľné z vonkajšej siete a sú tým pádom chránené pred útokmi z nej. Nie sú však chránené pred útokmi z demilitarizovanej zóny, preto sa všetky uzly demilitarizovanej zóny považujú za bastion hosty.

6 Firewally a operačné systémy

Keďže firewall môže byť softvérový – proces bežiaci na počítači alebo priamo zabudovaný v jadre operačného systému, nasledujúce časti hovoria o implementáciách firewallových možností v jednotlivých operačných systémoch.

6.1 Windows

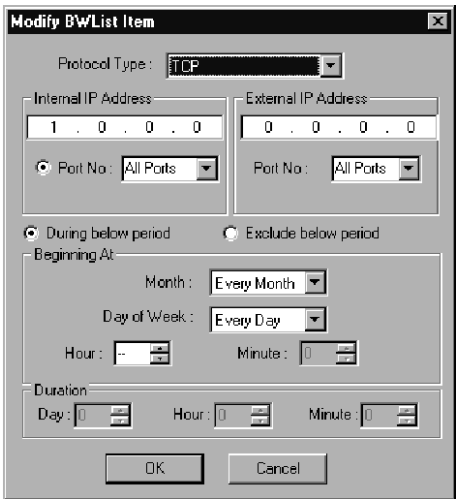
Operačný systém Windows 2000 má v inštalácii len jednoduchý filter prichádzajúcich paketov (obr. 11). Dokonca ani systémy série Windows 2000 Server na tom nie sú o nič



Obrázok 11: IP filtrovanie Windows 2000

lepšie. Ak chcete prevádzkovať firewall na Windowsoch, musíte využiť komerčné riešenia tretích firiem.

Ako príklad takéhoto riešenia uvádzam produkt SYGATE Home Network. Je to



Obrázok 12: Dialóg z programu Sygate Home Network

produkt určený pre malé siete. Obsahuje stavový paketový filtrer, proxy server, podporu IP smerovania vrátane NAT. Obrázok 12 ukazuje príklad konfiguračného dialógu tohoto programu.

6.2 Linux

V operačnom systéme Linux je priamo v jadre zabudovaný firewall. V závislosti od verzie jadra to je

- `ipfw` (Linux 2.0) – bezstavový paketový filter, pozná všetky protokoly založené na IP. Nevie pracovať s fragmentami.

- `ipchains` (Linux 2.2) – bezstavový paketový filter. Umožňuje spracovávať IP fragmenty, pozná NAT 1:N (masquerade). Umožňuje zvlášť konfigurovať pravidlá pre prichádzajúce, odchádzajúce, forwardované a maškarádované pakety.

- `iptables` (Linux 2.4) – stavový paketový filter.

Okrem paketových filtrov, ktoré bežia v móde jadra existuje pre Linux (a Unix všeobecne) veľké množstvo aplikačných proxy serverov pre snáď každý aplikačný protokol. Značná časť z nich sú voľne šíriteľné.

Ako príklad uvádzam nastavenie firewallu pomocou ipchains:

- `ipchains -P input REJECT` – nastavenie ,,default policy" čo nie je povolené, to je zakázané

- `ipchains -A input -s 192.168.0.0/24 -d 0.0.0.0/0 -i eth0 -j ACCEPT` – povolenie prevádzky z lokálnej eternetovej siete kamkoľvek

- `ipchains -A input -s 0.0.0.0/0 -p tcp -y -j REJECT` – zakázanie všetkých príchodzích tcp spojení

- `ipchains -A forward -s 0.0.0.0/0 -d 0.0.0.0/0 -i ppp0 -j MASQ` – nastavenie ppp adaptéra ako zariadenia, cez ktoré sa bude vykonávať masquerading

A Použitá literatúra

- Trusted Information Systems: TIS Internet Firewall Toolkit, overview.

- J. Ziegler: Firewally. Prednáška na konferencii Linuxový víkend. Bratislava 2001.

- M. Curtin, M.J. Ranum: Internet Firewalls – Frequently Asked Questions. 2000. `http://www.interhack.net/pubs/fwfaq`.

- AppGate: AppGate White Paper. `http://www.apgate.com`.

- Sygate: Home Network. Používateľská príručka. `http://www.sygate.com`.

- Linux Firewalling Howto.