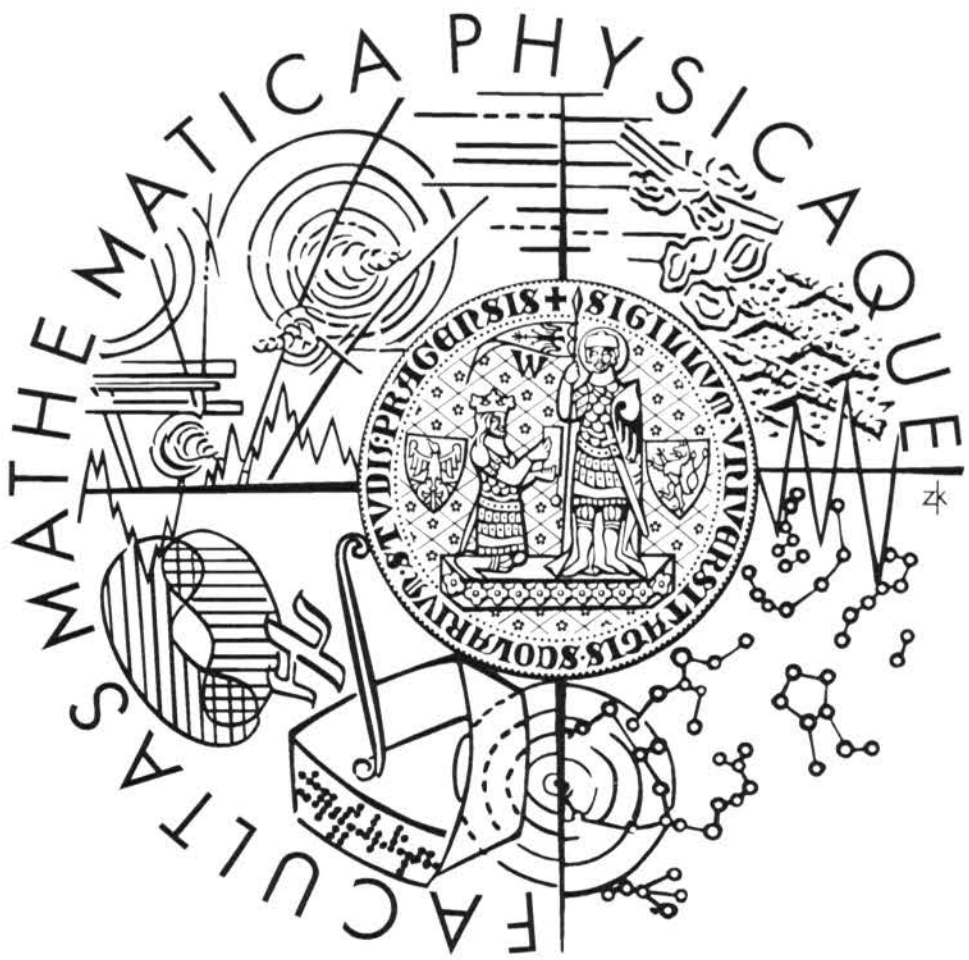
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Andrej Kalický

Firewall a internetová (síťová) bezpečnost

Katedra softwarového inženýrství

Vedoucí bakalářské práce: Doc. RNDr. Pavel Pyrih, CSc.,
Katedra matematické analýzy

Studijní program: Informatika, Správa počítačových systémů (ISPS)

2009

Rád by som poďakoval Doc. RNDr. Pavlovi Pyrihovi, CSc. za odborné vedenie a venovaný čas, taktiež za jeho cenné rady, nápady a pripomienky.

Prehlasujem, že som svoju bakalársku prácu napísal samostatne a výhradne s použitím citovaných prameňov. Súhlasím so zapožičiavaním práce a jej zverejňovaním.

V Prahe dňa 20.5.2009 Andrej Kalický

Obsah

Název práce: Firewall a internetová (síťová) bezpečnosť
Autor: Andrej Kalický
Katedra (ústav): Katedra softwarového inženýrství
Vedoucí bakalářské práce: Doc. RNDr. Pavel Pyrih, CSc.,
Katedra matematické analýzy
e-mail vedoucího: Pavel.Pyrih@mff.cuni.cz

Abstrakt: *V predloženej práci autor skúma internetovú a sieťovú bezpečnosť z hľadiska firewallu a identifikuje slabé a silné miesta zabezpečenia sietí. Vysvetľuje kľúčové pojmy akými sú bezpečnostná politika, bezpečnostné okruhy sietí, uvádza používané softwarové a hardwarové komponenty v podobe gateway a firewall. Popisuje vývoj a evolúciu firewallov z historického hľadiska, jednotlivé používané technológie firewallov, ich výhody a nevýhody vo vzájomnej konfrontácii. Z pohľadu architektúry sietí rozoberá možnosti zakomponovania firewallov do siete a pojednáva o ich efektívnom pôsobení. Snaží sa sumarizovať dané informácie a na ich základe naznačiť prognózu zabezpečenia sietí a bezpečnostnej politiky do budúcnosti.*

Klíčová slova: firewall, sieť, Internet, bezpečnosť, architektúra

Title: Firewall and Internet (net) security
Author: Andrej Kalický
Department: Department of Software Engineering
Supervisor: Doc. RNDr. Pavel Pyrih, CSc., Department of Mathematical Analysis
Supervisor's e-mail address: Pavel.Pyrih@mff.cuni.cz

Abstract: *In the propounded thesis author analyses Internet and net security from the point of view on firewall and identifies weak and strong points of net security. It explains the keywords as follows: security policy, security perimeter networks. It indicates used software and hardware components like gateway and firewall. It describes an evolution of firewalls from historical viewpoint, particular used firewall technologies, their advantages and disadvantages in mutual confrontation. In the term of network architecture it considers the options how to attach firewall into network and dissertates about their effective work. It tries to summarize the given information and based on their review denotes the future prognosis of net security and security policy.*

Keywords: firewall, network, Internet, security, architecture

Úvod

Samozrejmosťou nášho každodenného života sa stávajú počítače, smartphoney, informačné a telekomunikačné technológie. Bez týchto prostriedkov si existenciu už ani nevieme predstaviť. Stávame sa otrokmi vlastných vynálezov alebo naopak?

Na začiatku tretieho tisícročia väčšina spoločností verí, nehľadiac na ich veľkosť, že prístup k Internetu je nevyhnutný pri úspechu v konkurenčnom boji. Samozrejme s prospechom pripojenia prichádzajú aj riziká. Pripojenie privátnej siete k Internetu neznamená len, že pracovníci môžu pristupovať k externým informáciám a internetovým službám, ale zároveň za určitých podmienok a určitými prostriedkami sprístupniť externým užívateľov privátne informácie. Z tohto dôvodu každá spoločnosť zvažujúca pripojenie sa musí zaoberať otázkou internetovej a sieťovej bezpečnosti.

"Čo je firewall?", opýtal sa ma istého dňa otec demonštrujúc, že Internetová bezpečnosť už nie je len obor, týkajúci sa zopár "zasvätených", ale čoraz viac sa dotýka širokej verejnosti - koncových užívateľov. Odpovedal som mu, že zmysel činnosti firewallu spočíva zabrániť neoprávneným prístupom a zadržať útoky zlomyseľných užívateľov, aby neprenikli do našej vnútornej siete, serverov a osobných počítačov. Myslím, že táto jednoduchá a trefná odpoveď je pravdivá a nemenná. Čo sa však určite zmení a neustále technologicky vyvíja je to, ako firewall a iné zariadenia vykonávajú funkcie firewallu.

V tejto práci sa zameriavam na internetovú a sieťovú bezpečnosť, ktorej je venovaná prvá kapitola. Uvádzam v nej definície pojmov: bezpečnostná politika, bezpečnostné okruhy sietí, šifrovanie, gateway a firewall. Druhú kapitolu venujem firewallom, vývoju a evolúcii z historického hľadiska. Rozoberám používané technológie a metódy, ich výhody a nevýhody. Z pohľadu architektúry siete popisujem možné varianty zakomponovania firewall technológie a poukazujem na efektívnosť v jednotlivých prípadoch.

V tretej kapitole rozoberám aké služby a príslušné protokoly možno filtrovať a prečo. V štvrtej kapitole naznačujem, aká je vízia do budúcnosti na základe uvedených informácii a rozmanitých požiadaviek. Záver je venovaný zhrnutiu myšlienok a princípov používaných pri zabezpečovaní sietí, poukazujem aká je skutočnosť, ako sú zabezpečené spoločnosti a ako užívateľské počítače.

1 Bezpečnosť

Bezpečnosť a všeobecné pravdy o nej.

There is no such thing as absolute security.

Security is always a question of economics.

An attacker doesn't go through security, but around it.

A program or protocol is insecure until proven secure.

A chain is only as strong as its weakest link.

Security is a trade-off with convenience.

1.1 Bezpečnostná politika

Myšlienka vytvorenia bezpečnostnej politiky môže zaváňať byrokraciou. Pripomína hrubú knihu predpisov a pravidiel, ktoré musia byť prečítané, pochopené a dodržiavané.

Bezpečnostná politika je súbor rozhodnutí, ktoré kolektívne určujú postoj organizácie k bezpečnosti. Vymedzuje hranice akceptovateľného správania a reakciu pri ich porušení.

S návrhom bezpečnosti sa naskytujú nasledujúce otázky:

Aké zdroje sa pokúšame chrániť?

Kto má záujem na nás útočiť?

Aké rozsiahle bezpečnostné opatrenia si môžeme dovoliť?

1.2 Bezpečnostné okruhy [2]

Ak chceme definovať sieťovú bezpečnostnú politiku, musíme si zadefinovať metódy na zabezpečenie siete a jej obsahu, a taktiež užívateľov proti stratám a poškodeniu. Z tejto perspektívy, sieťová bezpečnostná politika hrá dôležitú úlohu v presadzovaní celkovej bezpečnostnej politiky definovanej spoločnosťou.

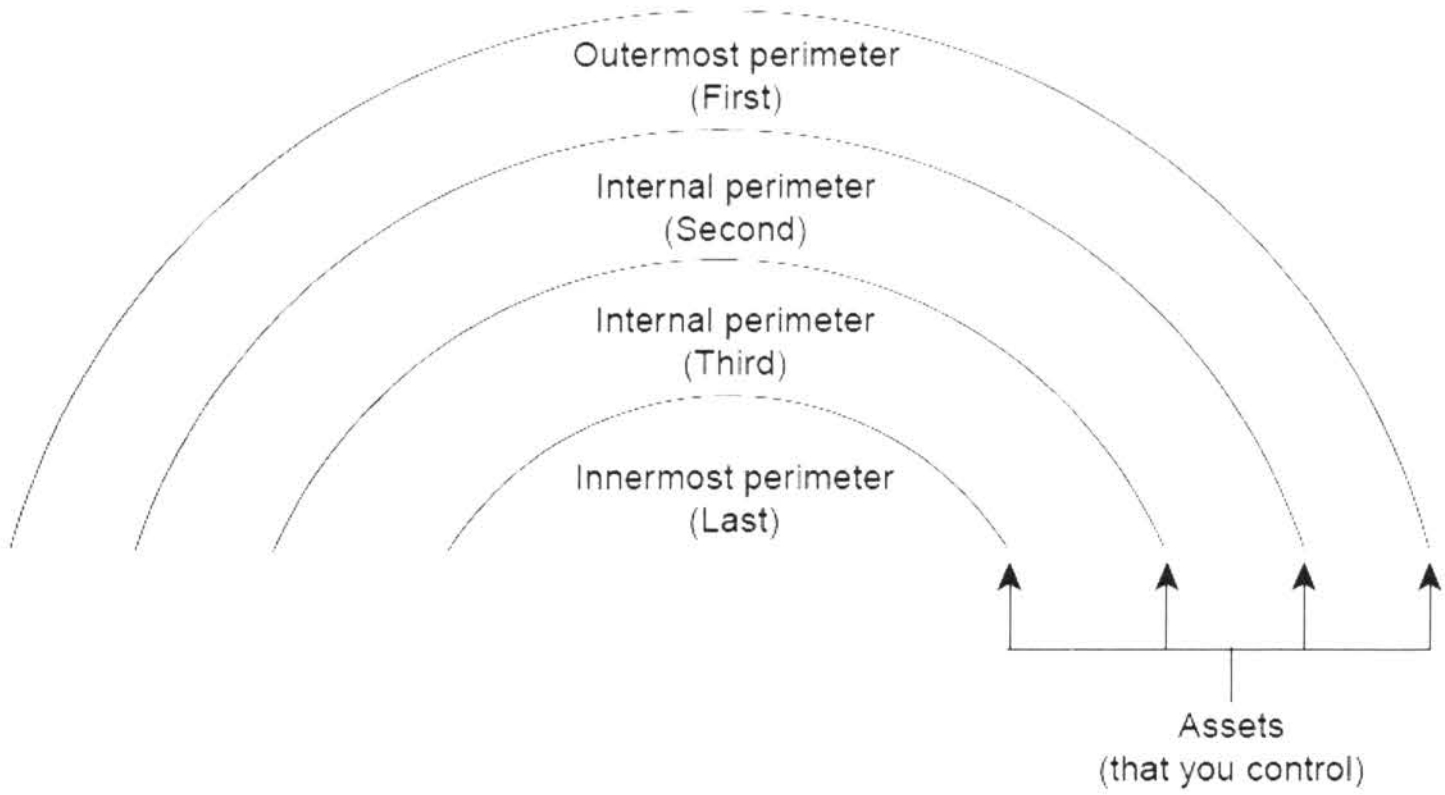
Sieťová bezpečnostná politika sa zameriava na kontrolu sieťového trafficu (sieťovej premávky) a jeho použitia. Identifikuje sieťové prostriedky a hrozby, definuje použite a zodpovednosť, detaily a plány v prípade porušenia bezpečnostnej politiky.

Pri navrhovaní sieťovej bezpečnostnej politiky, si treba strategicky určiť hranice a stupeň zabezpečenia na nich. Takéto strategické hranice v rámci siete sa nazývajú *perimeter networks.*

Perimeter Networks (okruhy sietí)

Perimeter Networks, alebo *okruhy sietí*, predstavujú vrstvový stupeň ochrany a zabezpečenia, a pomôžu nám v ujasnení o polohe firewallu v architektúre siete.

Na vytvorenie kolekcie bezpečnostných okruhov sietí, si musíme stanoviť počítačové siete, ktoré chceme chrániť, a definovať bezpečnostný mechanizmus na ochranu týchto sietí. K zvýšeniu bezpečnosti musí byť firewall server bránou pre každú komunikáciu medzi *trusted networks* na jednej strane a *untrusted* a *unkown networks* na druhej. Sledujeme tri typy okruhov: najokrajovejší (outermost), vnútorný (internal) a najvnútornejší (innermost).

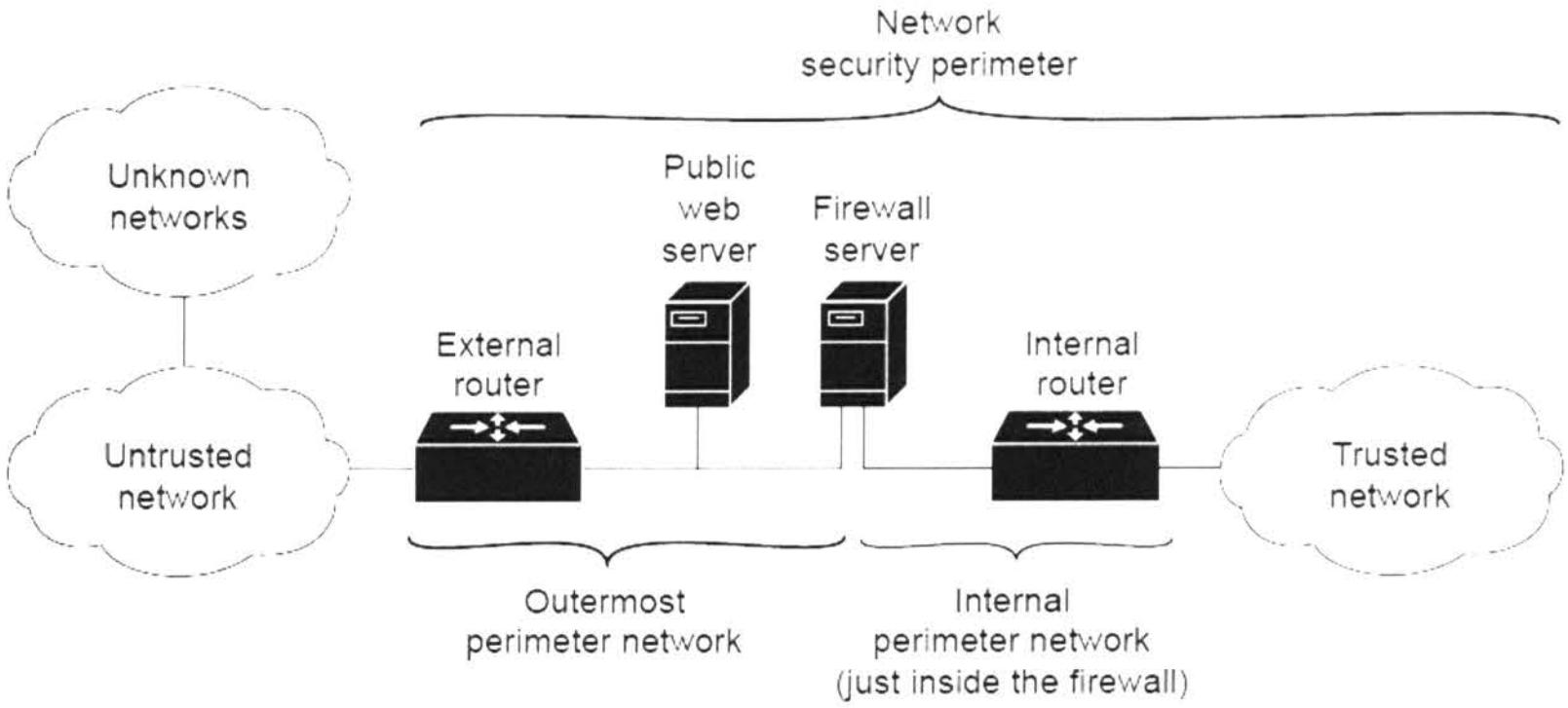


Obrázok 1.1: Okruhy sietí

Outermost perimeter network identifikuje oddeľujúci bod medzi prostriedkami, nad ktorými máme a nemáme kontrolu. Týmto bodom je router, ktorý separuje sieť od ISP network – siete poskytovateľa internetového pripojenia. Okruh býva normálne vyhradený pre routery, firewall servery a public web servery, ako HTTP a FTP servery. K tejto časti siete je ľahko získateľný prístup, preto býva často atakovaná, zvyčajne s pokusom získať prístup do internej siete.

Internal perimeter network reprezentuje ďalšie hranice, kde sú situované bezpečnostné mechanizmy, ako internet firewall a filtrujúce routery.

Na obrázku 1.2 je zobrazené umiestnenie vnútorného a vonkajšieho routera a firewall servera v súvislosti s okruhmi siete. Situovanie poskytuje malú dodatočnú ochranu voči útokom z oboch strán. Značne redukuje veľkosť trafficu, ktorý musí firewall server zhodnotiť. Zvýši sa tým výkon firewallu. Z pohľadu užívateľov na vonkajšej strane, server zastupuje všetky prístupné počítače v dôveryhodnej sieti. Je akýmsi hrdlom, cez ktoré prebieha komunikácia s vonkajšími sieťami.



Obrázok 1.2: Bezpečnostné okruhy sietí

Na základe spôsobu, akým Ethernet distribuuje a spracováva sieťové pakety, možno umiestnením filtrujúcich routerov okolo firewall serveru predísť k zaneprázdnenosti firewallu. V prípade absencie vnútorného filtrujúceho routera, musí firewall spracovať aj každý paket, ktorý je distribuovaný v rámci subnetu, alebo ak je paket určený pre ďalší vnútorný terminál.

Trusted Networks (dôveryhodné siete)

Navzájom dôveryhodné siete sú siete nachádzajúce sa vo vnútri sieťového bezpečnostného okruhu (network security perimeter). Tieto siete sa snažíme pomocou firewallov chrániť.

Pri nastavovaní firewall servera, sa explicitne identifikujú typy sietí, ktoré sú k nemu pripojené cez sieťové karty (network adapter card). Po počiatočnej konfigurácii dôveryhodné siete zahŕňajú firewall server a všetky siete za ním.

Výnimkou k obecnému pravidlu je zahrnutie *Virtual Private Network* (VPN) k dôveryhodným sieťam. Prenášajú dáta naprieč nedôveryhodnými sieťami (untrusted network). Pre komunikáciu vznikajúcu vo VPN musí existovať bezpečnostný mechanizmus, ktorým firewall server overuje pôvod, integritu dát a iné bezpečnostné princípy obsiahnuté na traffic v sieti. Uplatňujú sa rovnaké bezpečnostné princípy ako v dôveryhodnej sieti.

Untrusted Networks (nedôveryhodné siete)

Untrusted Networks, alebo nedôveryhodné siete, sa nachádzajú mimo bezpečnostného okruhu našej siete. Nemáme kontrolu nad ich administráciou a bezpečnostnou politikou, lebo tá sa na ne nevzťahuje. Práve preto je snaha zamedziť neoprávnenému prístupu

z nich. Avšak niekedy potrebujeme a chceme komunikovať s týmito sieťami, aj napriek tomu že sú nedôveryhodné.

Pri nastavovaní firewall servera sa explicitne identifikujú tie, od ktorých má firewall akceptovať požiadavky. Sú vonkajšie voči firewallu serveru.

Unknown Networks (neznáme siete)

Unknown Networks, alebo neznáme siete, sú siete, ktoré nie sú ani dôveryhodné ani nedôveryhodné. Sú neznámeho množstva, pre firewall ich nemožno explicitne identifikovať/zadať. Nachádzajú sa mimo bezpečnostného okruhu našej siete. (Štandardne všetky nedôveryhodné siete sú považované za neznáme.)

1.3 Internetová bezpečnosť [6]

V tejto sekcii rozoberiem principiálne možnosti zabezpečenia požiadaviek na identifikáciu, autentifikáciu, integritu, dôvernosť a (ne)odmietnuteľnosť. Najskôr spomeniem mechanizmy a technológie, ktoré sú dnes k dispozícii pre realizáciu týchto požiadaviek a uvediem niektoré spôsoby ich konkrétneho využitia.

1.3.1 Symetrické šifrovanie (Symmetric Cryptography)

Ide o techniku šifrovania, ktorá pracuje s dvoma identickými kľúčmi. Každý z nich je možné využiť rovnako pre zašifrovanie, ako aj pre odšifrovanie. Ak sa zabezpečí, aby odosielateľ a príjemca boli vybavení týmito kľúčmi (a nemal ich nikto iný), možno symetrické šifrovanie využiť najmä na zabezpečenie dôvernosti dát (bez potrebného kľúča ich nikto tretí "neodomkne"). Súčasne s tým môže byť splnená aj požiadavka na identifikáciu a autentifikáciu (protistranou je ten, kto má kľúč) aj na neodmietnuteľnosť (nikto iný ako vlastník kľúča nemohol údaje "zamknúť", t.j. zašifrovať) i integritu (nikto iný nemohol údaje "odomknúť", pozmeniť a zase znovu "zamknúť").

Symetrické šifrovanie je navyše výhodné v tom, že jeho výpočtová náročnosť nie je príliš veľká (aspoň v porovnaní s asymetrickým šifrovaním)[1].

Veľkou nevýhodou symetrického šifrovania je ale manipulácia s (identickými) kľúčmi, ktoré sa samozrejme nesmú dostať do nesprávnych rúk (preto sa aj hovorí, že ide o "tajný" kľúč). Ide hlavne o distribúciu týchto kľúčov, presnejšie o zabezpečenie toho, že tajný kľúč sa dostane práve a iba do rúk toho, kto má byť jeho vlastníkom (ak toto nie je splnené a tajný kľúč sa dostane do rúk niekoho iného, celé zabezpečenie sa stáva zbytočným) V praxi sa často používa fyzické odovzdanie tajného kľúča na vhodnom nosiči.

[1] samotná výpočtová náročnosť závisí od konkrétnej použitej šifrovacej metódy a požadovanej dĺžky kľúča

1.3.2 Asymetrické šifrovanie (Asymmetric Cryptography)

Pri tejto technike šifrovania sa pracuje s dvoma rôznymi kľúčmi, z ktorých len jeden musí zostať utajený (ako tzv. privátny kľúč), zatiaľ čo druhý kľúč nie je potrebné zachovať v utajení - práve naopak. Kvôli ľahšiemu využitiu celého asymetrického šifrovania, je vhodné ho uverejniť tak, aby bol každému ľahko dostupný (preto je aj tento kľúč označovaný ako "verejný"). S distribúciou takéhoto verejného kľúča potom nie sú žiadne problémy.

Podstatné pritom je, že to čo je "zamknuté" (zašifrované) jedným z kľúčov, možno "odomknúť" (odšifrovať) práve a iba len tým druhým z oboch kľúčov. Túto dôležitú vlastnosť asymetrického šifrovania možno využiť dvoma odlišnými spôsobmi:

Použitím privátneho kľúča k zašifrovaniu a verejného kľúča k odšifrovaniu. Keďže privátny kľúč má k dispozícii iba jeho oprávnený vlastník, môže toto urobiť len on. Naproti tomu verejný kľúč má k dispozícii v zásade každý, takže odšifrovanie môže realizovať podobne každý.

Výsledkom je splnenie požiadaviek na identifikáciu a autorizáciu (pretože nikto iný ako skutočný autor nemohol dáta zašifrovať privátnym kľúčom), ďalej požiadavky na integritu (nikto iný nemohol údaje odšifrovať, zmeniť a opäť zašifrovať privátnym kľúčom), aj na neodmietnuteľnosť (údaje nemohol zašifrovať nikto iný ako vlastník privátneho kľúča).

Za zdôraznenie určite stojí, že týmto spôsobom nie je splnená požiadavka na dôveryhodnosť - vzhľadom k verejnému charakteru kľúča sa k dátam môže dostať skutočne ktokoľvek.

Pomocou verejného kľúča na zašifrovanie a privátneho kľúča k odšifrovaniu. Keďže k verejnému kľúču má prístup ktokoľvek, môže zašifrovanie vykonať taktiež ktokoľvek. Vskutku odšifrovať takto zašifrované údaje môže iba vlastník privátneho kľúča a nikto iný.

To v praxi znamená naplnenie požiadavky na dôvernosť (nikto iný ako vlastník privátneho kľúča ich nemôže "odomknúť", t.j. odšifrovať). Naproti tomu tu nie je splnená ani požiadavka na autentifikáciu a neodmietnuteľnosť (zašifrovať mohol ktokoľvek).

Požiadavka na integritu v podstate tiež nie je splnená, pretože ktokoľvek mohol pôvodné dáta zahodiť (nemôže ich odšifrovať), a nahradiť ich vlastnými dátami, korektne zašifrovanými verejným kľúčom.

1.3.3 Jednorazové heslá (One-Time Password)

Heslá sa používajú obvykle hlavne na autentifikáciu a pre potreby autorizácie.

Ak sú tieto heslá prenášané nezabezpečeným spôsobom po nezabezpečenej sieti, alebo sú zverované subjektom, ktorí nemusia byť úplne dôveryhodní, hrozí možnosť

ich zneužitia (odpočúvanie, kopírovanie alebo iné "prezradenie" a následné nelegitímne použitie).

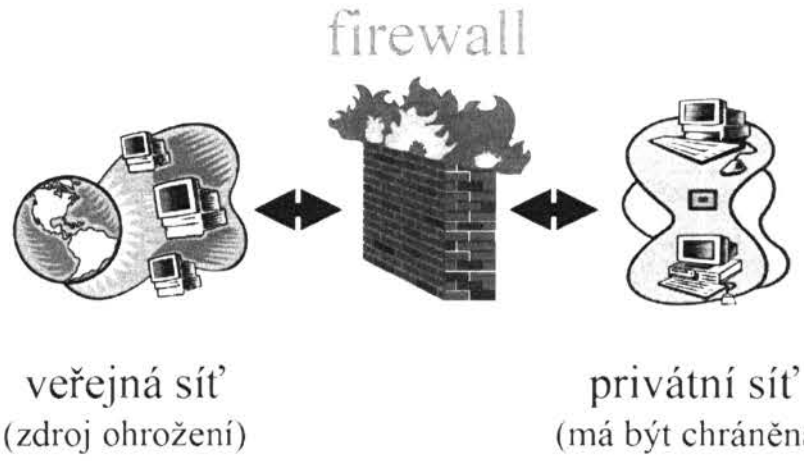
Jednou zo zaujímavých možností je použitie takýchto hesiel, ktoré majú iba jednorazovú platnosť, pre jeden jediný úkon, a ich prípadné vyzradenie potom nie je nebezpečné (pretože ich nemožno použiť opakovane). Príkladom je potvrdzovanie transakcií pre internetové bankovníctvo, keď Vám informačný systém zašle jednorazové heslo prostredníctvom SMS.

Nevýhodou je spôsob generovania takýchto jednorazových hesiel, ktorý zvyčajne vyžaduje dopraviť k oprávnenému používateľovi vhodný generátor (či už v podobe programu, ktorý si dotyčný inštaluje na svoj počítač, alebo v podobe fyzického zariadenia).

1.4 Gateway a Firewall

Firewall pôvodne podľa slovníka, označuje ohňovzdornú fyzickú stenu používanú ako bariéru proti šíreniu ohňa a tepla.

Firewall, je sieťové zariadenie, software, opatrenie alebo vybavenie, ktoré slúži k zabezpečeniu sieťovej prevádzky a prístupu. Slúži ako kontrolný bod, ktorý definuje pravidlá pre komunikáciu medzi sieťami. Chráni jednu sieť pred ostatnými. Zvyčajne, firewall chráni/oddeľuje privátnu sieť (private network) pred verejnou (public) alebo zdieľanou (shared), ku ktorej je pripojená.[2]



Obrázok 1.3: Firewall

Pravidlá pre komunikáciu historicky vždy zahrňovali identifikáciu zdroja a cieľa dát (zdrojovú a cieľovú IP adresu) a zdrojový a cieľový port, čo je však už pomerne nedostatočné. Modernejšie firewally sa opierajú o informáciu o stave spojenia, znalosť kontrolovaných protokolov a prípadne prvky IDS (Intrusion Detection System).

Gateway alebo v preklade termín *brána*, môže byť interpretovaný rôzne. Niekedy je tento pojem používaný ako spoločný zastrešujúci termín pre všetky ostatné termíny. Napríklad v tom zmysle, že smerovač je taká brána, ktorá pracuje na úrovni sieťovej vrstvy.

V užšom slova zmysle sa ale *bránou* rozumie také zariadenie, ktoré pracuje na úrovni ešte vyššej, ako je vrstva sieťová (t.j. na transportnej až aplikačnej vrstve).

Pre správne pochopenie významu brán je dobré si uvedomiť jednu dôležitú skutočnosť: počítačové siete nie sú všetky rovnaké. Práve naopak, často sa môžu aj veľmi výrazne líšiť. Na tom, ako ďaleko sa líšia, potom závisia aj možnosti ich prepojenia na úrovni jednotlivých vrstiev. Všeobecne platí, že čím väčšia je odlišnosť, tým vyššia je vrstva, na ktorej je možné realizovať ich vzájomné prepojenie.

Z tohto pohľadu potom *brána* slúži na prepájanie tých najviac odlišných sietí. Veľmi často pracujú brány až na aplikačnej vrstve, kde zabezpečujú prenos dát medzi jednotlivými aplikáciami.

Príkladom môžu byť rôzne druhy poštových brán (mail gateways), ktoré umožňujú posielať elektronickú poštu z jednej siete do druhej. Rôzne siete totiž môžu používať rôzne formáty jednotlivých správ (hlavne hlavičky), iný spôsob adresovania, a napríklad aj iný spôsob kódovania jednotlivých znakov v tele i hlavičke správy. Zabezpečiť potrebnú konverziu potom dokáže až brána, pracujúca na aplikačnej úrovni, pretože iba na tejto úrovni môže "vnímať" štruktúru prenášaných dát, a dokáže tak rozpoznať jednotlivé správy a správne interpretovať (a skonvertovať) ich obsah.

Pre brány, pracujúce na nižšej úrovni, by išlo len o súvislý prúd dát, ktorých význam by na tejto úrovni už nebol známy.[5]

DMZ

Niektorým serverom je obtiažne dôverovať kvôli veľkosti a komplexnosti ich kódu. Web servery sú klasickým príkladom. Umiestniť ich za firewall alebo pred? Ak sú umiestnené vo vnútri siete, tak potom prípadným zneužitím server vytvára spúšťací bod pre ďalšie útoky na vnútorné počítače. Umiestnením mimo privátnej siete sa stávajú servery ľahšie napadnuteľné.

Bežným spôsobom je vytvoriť *delimitarizovanú zónu*[2] medzi dvomi firewallmi. Ako aj v skutočnom svete, analogicky v Kórei, pásmo DMZ je potrebné pozorne monitorovať. Je to miesto, kde sú citlivé objekty vystavené vyššiemu riziku ako služby, ktoré sú iba vo vnútri.[1]

Celková premávka cez DMZ je zablokovaná. Hlavnou myšlienkou je umiestniť do DMZ prestupné stanice, cez ktoré je premávka povolená a účinne kontrolovateľná. Prestupné stanice sú v skutočnosti aplikačné brány špecializované na určitý druh premávky, napríklad WWW, FTP, DNS servery, prestupný poštový server.[4]

[2] v skutku ju môžeme chápať ako "zem nikoho"

Obrázok 1.4: Demilitarizovaná zóna medzi dvoma smerovačmi

DMZ je vidieť z oboch strán, ale nie je priehľadná skrz. Z nechránenej siete (Internetu) vidno iba uzly priamo v DMZ. Celá chránená sieť je zvonku neviditeľná. Môže tak používať aj adresy, ktoré by boli vonku neprístupné.[4]

Prečo by sme nemali dôverovať staniciam, ktoré sú umiestnené v DMZ? To je dôvod prečo sme ich tam umiestnili. *Nič* nie je kompletne bezpečné, ale niektoré situácie vyžadujú väčšiu starostlivosť a ochranu ako ostatné.

2 Firewally

2.1 História vývoja

Firewall technológia sa objavila koncom 80tych rokov, keď Internet predstavoval úplne novú technológiu v zmysle jej globálneho použitia a pripojenia. Predchodcom firewallov v sieťovej bezpečnosti boli smerovače používané na konci 80tych rokov na oddelenie sietí. V ranných rokoch, Internet podporoval relatívne malú komunitu kompatibilných používateľov, ktorí oceňovali otvorenosť pre zdieľanie a spoluprácu. Pôvodná myšlienka pre vznik firewallov bola reakciou na množstvo významných internetových bezpečnostných prelomov:

- Clifford Stoll objavil Nemeckých špiónov manipulovaním s jeho systémom. Poznatky publikoval v *Stalking the wily hacker*, v roku 1988.
- *Evening with Berferd* 1992 od Billa Cheswicka, kde nastavil jednoduché elektronické väzenie na sledovanie útočníkov.[7]
- V roku 1988, zamestnanec NASA Ames Research Center v Kalifornii poslal informáciu emailom jeho kolegovi, kde stálo:

  > *Sme aktuálne pod útokom internetového VIRUSu! Zasiahol Berkley, UC San Diego, Lawrence Livermore, Stanford a NASA Ames.*

- Červ Morris sa rozšíril cez viaceré zraniteľné miesta v staniciach času. Hoci nebol zlomyselný zámerne, ale bol prvým rozsiahlym útokom na internetovú bezpečnosť. Komunita takýto útok nečakala, a ani nebola pripravená sa s ním vyrovnať.[8]

Prvá generácia

Prvý dokument o firewall technológii bol publikovaný v 1988, keď Dodong Sean James a Elohra z Digital Equipment Corporation (DEC) vyvinuli filtrujúci systém - *packet filter firewalls*. Tento vskutku základný systém bol prvou generáciou, ktorá sa stala vysoko rozvinutou a technicky internetovou bezpečnostnou charakteristikou.

V AT&T Bill Cheswick a Steve Bellovin pokračovali v ich výskume paketového filtrovania. Vyvinuli fungujúci model pre ich vlastnú spoločnosť založený na ich prvotnej architektúre prvej generácie.[8]

Paketové filtre pôsobia skúmaním paketov, ktoré reprezentujú základnú jednotku dátového prenosu medzi počítačmi na Internete. Ak paket neodpovedá nastaveným pravidlám, je zahodený (tiché odhodenie), alebo odmietnutý (odhodený, a súčasne poslaná chybová notifikácia ku zdroju).

Tento typ filtrovania nezohľadňuje fakt, či paket je súčasťou existujúceho streamu premávky. Filtrovanie je založené len na informáciách obsiahnutých v pakete (source and destination address, protocol, port number - TCP and UDP traffic).

Druhá generácia

V rokoch 1989-1990 traja kolegovia z AT&T Bell Laboratories, Dave Presetto, Howard Trickey a Ksihitij Nigam vyvinuli druhú generáciu firewallov nazvanú *Circuit Level Firewall*.[8]

Taktiež implementovali prvý pracujúci model tretej generácie firewall architektúr. Bohužiaľ, nepublikovali žiaden dokument opisujúci túto architektúru a ani nevydali žiaden produkt založených na ich práci.[2]

Táto technológia je všeobecne označovaná ako *stateful packet inspection* (SPI) alebo *stateful firewall*. Udržuje záznamy o všetkých spojeniach prechádzajúcich cez firewall. Je schopná určiť, či je paket začiatkom novej komunikácie, súčasť už existujúcej komunikácie alebo je neplatný.

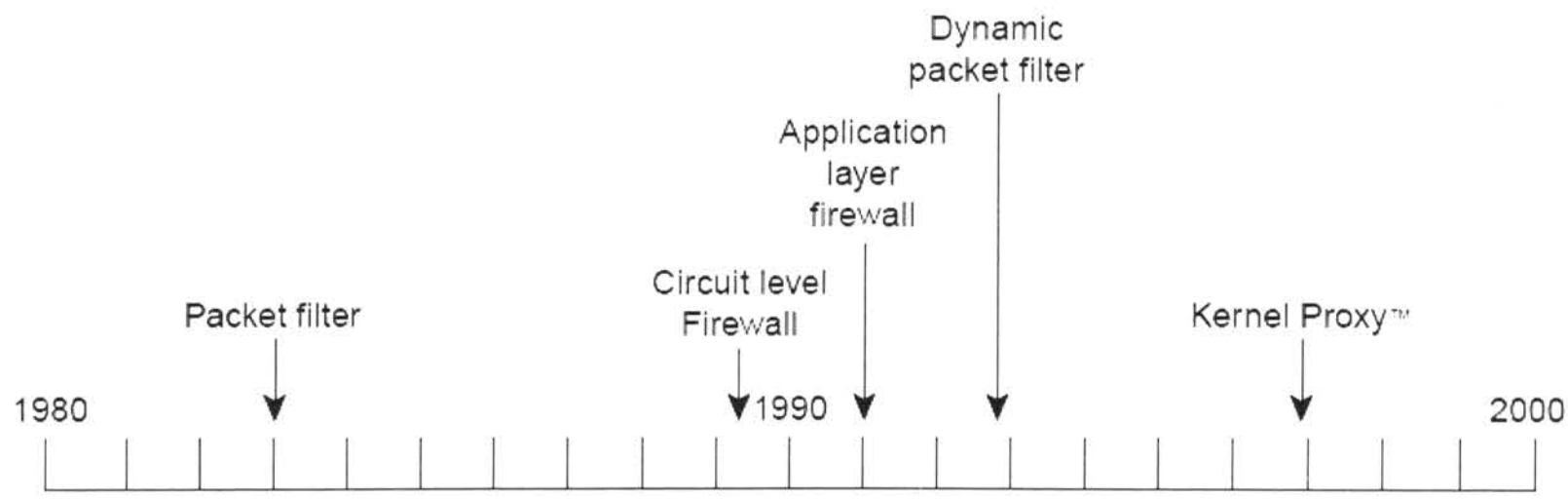
Stále však záleží na statických pravidlách v takýchto firewalloch, stav spojenia môže byť samo o sebe jedným z kritérií, ktoré spúšťajú osobitné pravidlá.

Tretia generácia

Ako sa často stáva v prípade výskumu a vývoja, tretia generácia firewall architektúr bola nezávisle vyvíjaná niekoľkými ľuďmi naprieč USA v neskorých 80tych a na začiatku 90tych rokov. Publikátormi boli Gene Spatfford z Purdue University, Bill Cheswick z AT&T Bell Laboratories a Marcus Ranum. Popísali *application level firewalls* (aplikačné firewally), tiež známe ako *proxy firewally*.

V roku 1991 najväčšiu pozornosť pútala práca Marcusa Ranuma, ktorá nadobudla formu obrannej stanice[1] s bežiacimi proxy službami. Jeho práca rýchlo vyústila do

[1] v literatúre používane aj názvy "bastion host" alebo "gateway"



Obrázok 2.1: História

prvého komerčného produktu - SEAL od spoločnosti Digital Equipment Corporation (DEC).[2]

TIS, v rámci širšieho kontraktu s DARPA, vyvinul *Firewall Toolkit* (FWTK) a urobil ho licenčne voľne dostupným 1. Októbra 1993. FWTK bol, a je, voľne dostupný vo forme zdrojového kódu pre výskum.[9]

Dôvody pre vydanie voľne k dispozícii, a nie pre komerčné využitie boli:

- demonštrovať (softvérom, dokumentáciou a použitými metódami) ako spoločnosť (v tej dobe) s 11-ročnými skúsenosťami s formálne bezpečnostnými metódami a fyzické osoby so skúsenosťami s firewallmi, dokázali vyvinúť firewall softvér
- vytvoriť spoločný základ veľmi dobrého firewall softvéru pre ostatných na nadviazanie vývoja (tak aby ľudia nemuseli pokračovať vo vlastnom implementovaní od nuly)
- zvyšovať úroveň používaného firewall softvéru

Medzi kľúčové výhody filtrovania na aplikačnej úrovni patrí schopnosť porozumieť určitým aplikáciám a protokolom (ako FTP, DNS, web browsing) a možnosť detegovať či nechcený protokol sa nezakráda neštandardným portom alebo či protokol nie je zneužitý škodiacim spôsobom.

Nasledujúci vývoj

Okolo roku 1991, Bill Cheswick a Steve Bellovin začali výskum s *dynamic packet filtering* a pokračovali, pokiaľ to bolo užitočné, v zdokonaľovaní interného produktu v Bell Laboratories, založeného na tejto architektúre. Avšak tento produkt nebol nikdy uvedený na trh.

V roku 1992, Bob Branden a Annette DeSchon na University of Southern California nezávisle zdokonaľovali koncept firewallu. Produkt, známy ako *Visas*, bol prvým systémom, ktorý mal vizuálne integrované rozhranie s ikonkami. Jednoducho implementovateľný a prístupný na počítačoch s operačným systémom ako Microsoft Windows alebo Apple MacOS.[2]

V roku 1994, izraelská spoločnosť Check Point Software Technologies uviedla na trhový komerčný produkt založený na štvrtej generácií architektúry firewallu pod názvom *FireWall-1*.[8]

Počas roku 1996, Scott Wiegel, hlavný vedec v Global Internet Software Group Inc., založil plány pre piatu generáciu architektúr firewallu - *Kernel Proxy* technológiu.

Jedna z najväčších spoločností, zaoberajúca sa internetovou bezpečnosťou, uviedla v roku 1997 prvý komerčný produkt *Cisco Centri Firewall* založený na tejto architektúre.[2]

Niektoré moderné firewally svoju hĺbkovú paketovú kontrolu zdieľajú s *Intrusion Prevention System*[2].[8]

V súčasnosti pracuje na štandardizovaní protokolov spravujúcich firewallmi a inými middleboxami skupina Middlebox Communication Working Group v rámci Internet Engineering Task Force (IETF).

[2]je sieťové bezpečnostné zariadenie, ktoré monitoruje sieť a/alebo systémové aktivity pre zlomyseľné a nechcené správanie. Môže reagovať v reálnom čase blokovaním alebo zabránením takýmto aktivitám.

2.2 Typy firewallov [1, 2, 12, 13]

Viac technológii firewallov poskytuje odlišnú schopnosť pre kontrolu komunikačných udalostí. Zvyčajne generujú audit záznamy popisujúce príčinu a okolnosti spustenia udalosti. Ako sa technológia zdokonaľovala, firewally dokázali preskúmať prídavné sieťové informácie v pakete používajúc viac vyspelejšie inšpekčné metódy.

2.2.1 Packet Filters (paketové filtre)

Paketové filtre, ako prvá generácia firewallov, analyzujú sieťovú premávku na úrovni transportnej vrstvy. Každý IP paket je skúmaný či vyhovuje jednému z množiny pravidiel definujúcich, ktoré dáta sú povolené. Pravidlá identifikujú či komunikácia je povolená na základe informácie obsiahnutej v hlavičke paketu a tiež smeru, ktorým je paket určený (prichádzajúci, odchádzajúci). Filtrovanie prebieha buď na prichádzajúcom rozhraní, na odchádzajúcom rozhraní alebo na oboch zároveň. Administrátor vytvorí zoznam počítačov a služieb, ktoré sú, alebo nie sú akceptovateľné pri komunikácii.

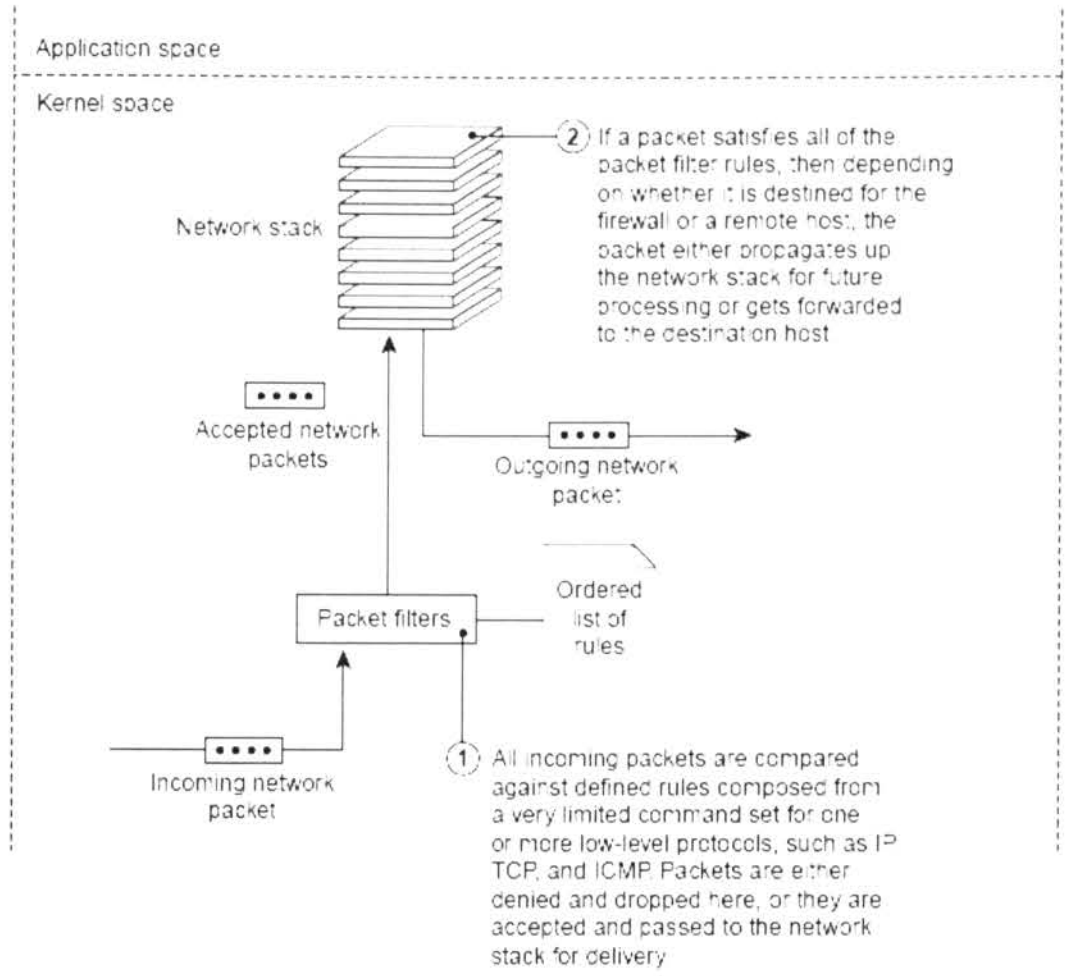
Paketové filtre typicky umožňujú zaobchádzať s prenosom dát opierajúc sa o:

- fyzická sieťová adresa, na ktorú paket prichádza
- zdrojová IP adresa, z ktorej bol paket (pravdepodobne) odoslaný
- cieľová IP adresa, pre ktorú je paket určený
- typ protokolu na úrovni transportnej vrstvy
- zdojový port, z ktorého paket prichádza
- cieľový port, na ktorý je paket určený

Na obrázku 2.2 je zobrazený proces vyhodnotenia paketovým filtrom. Architektúra implementuje limitované množstvo príkazov na vykonanie analýzy pre jeden alebo viac sieťových (IP) alebo transportných protokolov (TCP). Funguje na úrovni kernelu (jadra).

Paketové filtre obecne nerozumejú protokolom na úrovni aplikačnej vrstvy používaným v komunikačných paketoch, napr. FTP. Pracujú aplikovaním pravidiel udržovaných v TCP/IP jadre. K pravidlám sú priradené akcie, ktoré sa aplikujú na pakety vyhovujúce kritériám.

Akcia môže nadobúdať dve hodnoty: ***deny*** *(zamietnuť)* alebo ***permit*** *(povoliť)* sieťový paket. V jadre sú uchovávané 2 zoznamy: deny list a permit list. Aby bol paket smerovaný k správnemu cieľu, musí najskôr prejsť kontrolou cez oba zoznamy. Niektoré typy paketových filtrov, ktoré sú vstavané do routerov, implementujú odlišnú politiku. V týchto typoch musí byť paket jednoznačne zamietnutý, inak je povolený.



Obrázok 2.2: Paketový filter

Paketový filter typicky implementuje sadu príkazov, ktoré poskytujú kontrolu zdrojových a cieľových čísel portov na TCP a UDP transportných protokoloch. Zisťuje, či je pravidlo použiteľné pre kombináciu portu a protokolu. Naopak ICMP protokol nevyužíva čísla portov, filtrácia je obtiažnejšia. Na aplikovanie bezpečnostnej politiky na ICMP musí filter využívať *state table*. Schopnosť viesť *state* komunikáciu je základný rozdiel medzi jednoduchými paketovými filtrami a dynamickými paketovými filtrami.

Dômyselnejšie filtre sú schopné detegovať IP, TCP, UDP a ICMP. Možno povoliť určitý typ spojenia pre skupinu počítačov a zároveň zakázať ostatné typy spojení.

Úplná inšpekcia protokolov sa riadi podľa nasledujúceho algoritmu:

- Ak nie je nájdené žiadne odpovedajúce pravidlo, sieťový paket je zahodený.
- Ak je nájdené odpovedajúce pravidlo, ktoré povoľuje komunikáciu, potom je povolená peer-to-peer komunikácia.
- Ak je nájdené odpovedajúce pravidlo, ktoré zamieta komunikáciu, sieťový paket je zahodený.

Riešenie je najmenej bezpečné z pomedzi architektúr firewallov.

Routing Filters (smerovacie filtre)

Je dôležité filtrovať smerovacie informácie. Dôvod je prostý: Ak je uzol úplne nedosiahnuteľný, rovnako ako je odpojený od siete. Jeho bezpečnosť je takmer dobrá, ale nie

celkom. Ak sprostredkujúci uzol, ktorý ho môže dosiahnuť, je dosiahnuteľný z Internetu, potom údajne nedosiahnuteľný uzol môže byť následne zasiahnutý.

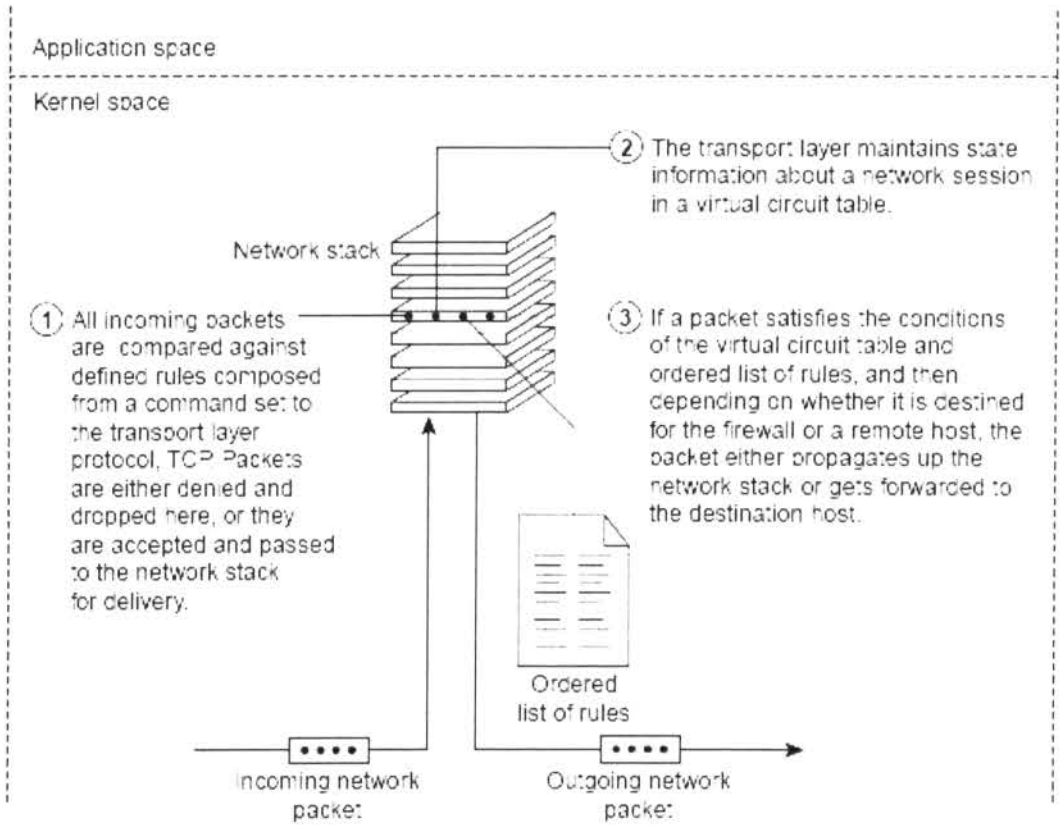
V situácii, keď klient využíva *IP source routing*, môže byť taktiež zdanlivo nedosiahnuteľný uzol zasiahnutý.

Route filtering môžeme docieliť aj takto: Úmyselne sa použijú neoficiálne IP adresy vnútri firewallu, prípadne môžu patriť niekomu inému. Pakety smerované na tieto adresy idú potom niekam inam. Táto metóda sa nazýva *route squatting*.

2.2.2 Circuit Level Firewalls (Stavové paketové firewally)

Circuit Level Firewall, alebo *stavový paketový firewall*, je druhou generáciou firewall technológie. Zohľadňuje fakt, či paket je požiadavka o spojenie alebo dátový paket patriaci spojeniu, prípadne virtuálnemu okruhu medzi dvoma príslušnými transportnými vrstvami.

Na overenie *session* (relácie) firewall skúma každé zostavenie spojenia zaisťujúc, či bol použitý legitímny *handshake*[3] pre transportný protokol. Dáta nie sú doručované až pokiaľ handshake nie je kompletný. Firewall si udržuje tabuľku platných spojení (vrátane *session state* - stavu relácie a sequencing information - sledu informácii) a necháva sieťové pakety obsahujúce dáta prechádzať, keď informácie paketu odpovedajú záznamu vo virtuálnej tabuľke okruhov. Akonáhle je spojenie prerušené, príslušný záznam je odstránený a virtuálny okruh uzavretý.[2]



Obrázok 2.3: Stavový paketový firewall

[3]metóda, pri ktorej sú prenášané signály tam a späť cez komunikačnú sieť, na založenie platného spojenia medzi dvoma stanicami

Tento typ firewallu analyzuje pravidlá pre spojenie založené na transportných protokoloch, zvyčajne iba TCP. Proces vyhodnocovania sieťového paketu stavovým paketovým firewallom je zobrazený na obrázku 2.4.

Keď je spojenie vytvorené, circuit level firewall typicky uchováva nasledujúce informácie o spojení:

- jedinečný session identifikátor pre spojenie, používaný na stopovacie účely
- stav spojenia: *handshake*, *established* alebo *closing*
- sequencing information - usporiadanie informácii
- zdrojová IP adresa, z ktorej bol paket odoslaný
- cieľová IP adresa, pre ktorú je paket určený
- fyzické sieťové rozhranie, cez ktoré paket prichádza
- fyzické sieťové rozhranie, cez ktoré paket odchádza

S použitím týchto informácií, firewall kontroluje hlavičky obsiahnuté v každom zo sieťových paketov, a rozhoduje či vysielajúca stanica má povolenie posielať dáta na prijímajúcu stanicu a či aj prijímajúca stanica má povolenie prijímať dáta.

Circuit level firewally povoľujú prístup cez firewall s minimálnym množstvom skúmania budujúc stav spojenia. Iba tie sieťové pakety, ktoré sú asociované s existujúcim spojením majú povolený prístup. Keď je prijatý paket so žiadosťou na vytvorenie spojenia, firewall overí pravidlá, či by mohlo byť spojenie povolené. Ak je povolené, všetky sieťové pakety asociované so spojením sú smerované cez firewall bez ďalšej bezpečnostnej kontroly. Táto metóda je veľmi rýchla, pretože zahŕňa menej vyhodnocovania a poskytuje obmedzený počet kontroly stavu.

Tento typ firewallov taktiež môže vykonávať dodatočnú kontrolu na zaistenie, že pakety neboli *spoofnuté* a dáta obsiahnuté v hlavičke odpovedajú definícii pre daný protokol.

Circuit level firewally často menia adresu paketov tak, že odchádzajúca komunikácia sa javí, že má pôvod u firewallu a nie u vnútornej stanice. Tento proces prepisovania adries paketov sa nazýva *Network Address Translation*. A pretože tieto firewally udržujú informácie o každej session, tak môžu vhodne mapovať externé odpovede spätne na príslušné vnútorné stanice.[2]

Medzi nevýhody Circuit level firewallov patria nasledujúce:

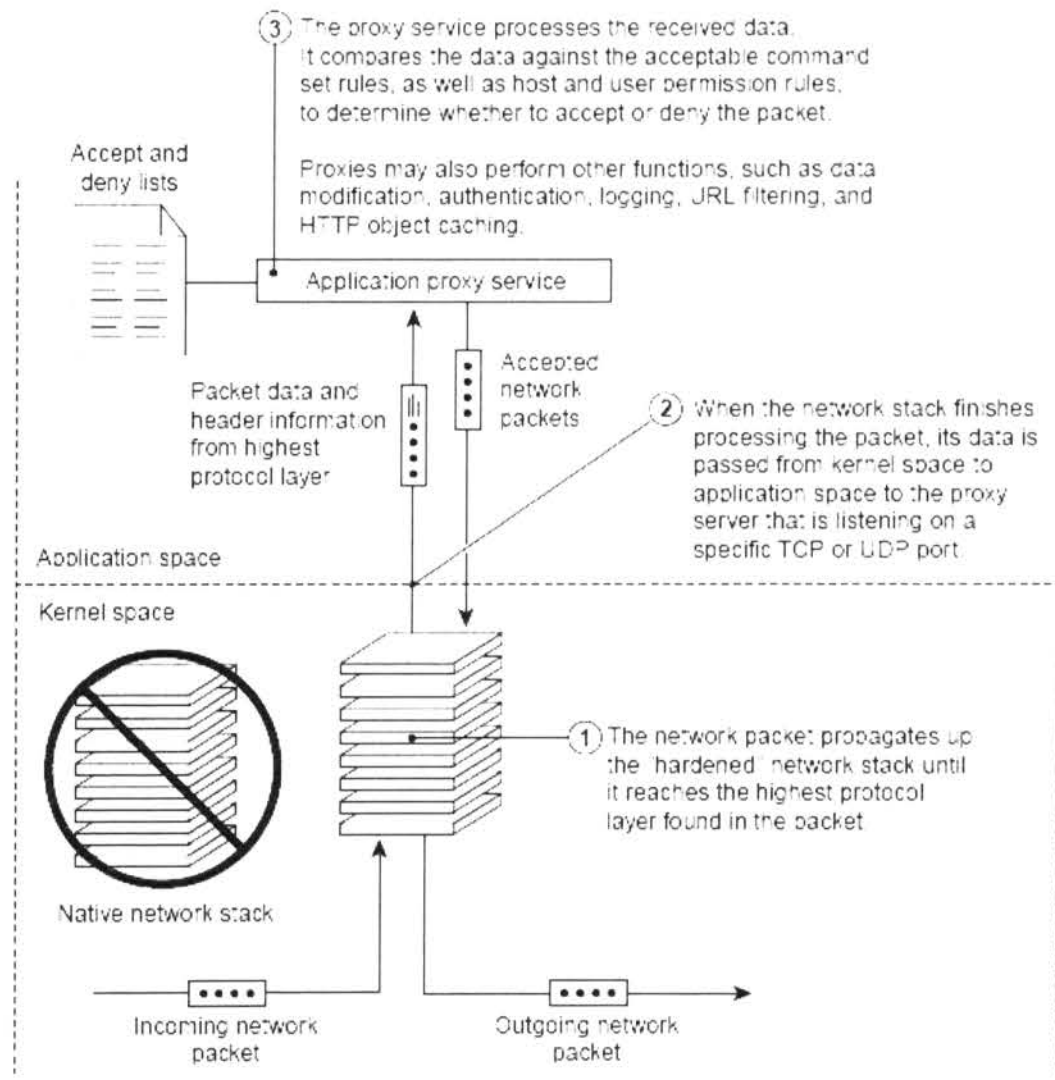
- Nemôžu vykonávať prísnu bezpečnostnú kontrolu na protokoloch vyšších vrstiev.

- Neponúkajú prídavné charakteristiky, ako napríklad HTTP object caching, URL filtrovanie a autentifikáciu.

- Obtiažne testovanie *accept* a *deny* pravidiel.

2.2.3 Application Layer Firewalls (Aplikačné firewally)

Application Layer Firewall, alebo *aplikačný firewall*, je firewall operujúci na aplikačnej vrstve *protocol stacku*[4]. Obecne využíva rozličné druhy proxy serverov na sprostredkovanie komunikácie namiesto smerovania. Môže preskúmavať obsah trafficu, blokovať nevhodný obsah, určité web stránky, vírusy, pokusy o preniknutie známymi logickými trhlinami v klientskom softvéri.



Obrázok 2.4: Aplikačný filter

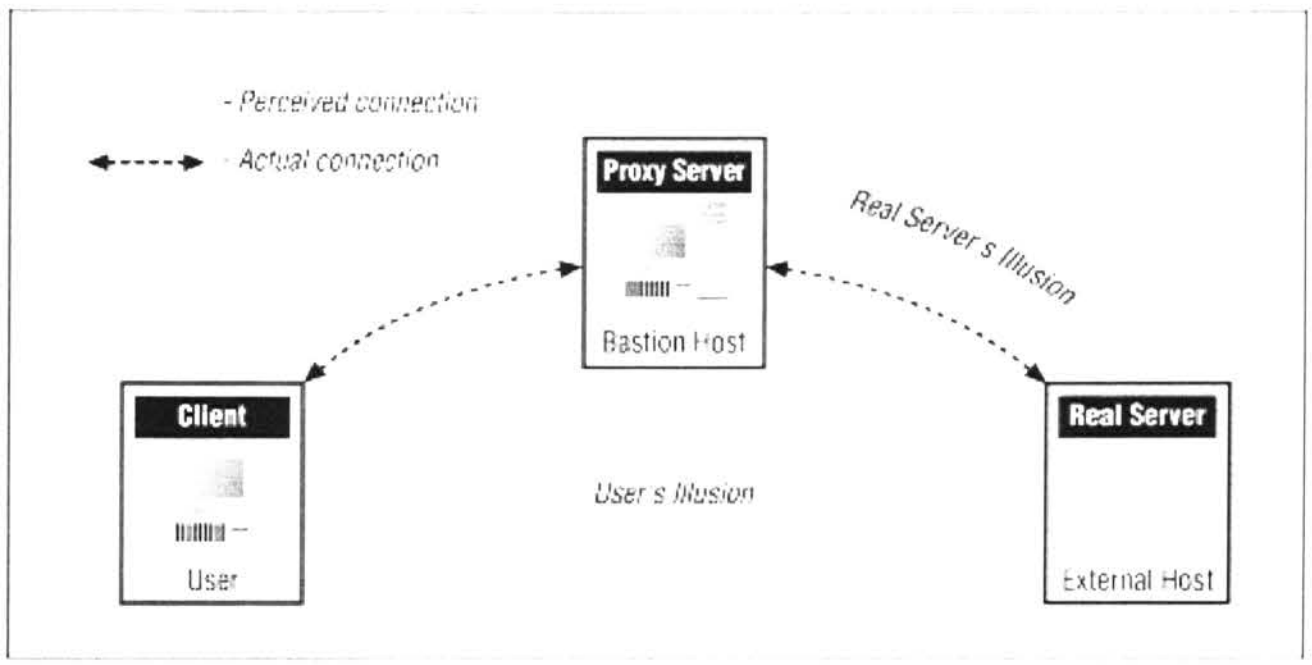
Aplikačný firewall, ako tretia generácia firewallov, kontroluje dáta vo všetkých sieťových paketoch na aplikačnej úrovni a podporuje kompletné stavové spojenie a usporiadanie informácií. Navyše môže overiť ďalšie bezpečnostné položky, ktoré sa objavia medzi aplikačnými dátami (užívateľské heslá, žiadosti služieb ...).[2]

Na obrázku 2.4 je zobrazený proces vyhodnocovania sieťového paketu aplikačným firewallom. Táto architektúra analyzuje pravidlá pre jednotlivý protokol v aplikačnom priestore.

[4]je detailná softvérová implementácia súboru komunikačných a počítačových sieťových protokolov; súbor je definícia protokolov a stack je ich implementácia

Proxy Services [2]

Väčšina aplikačných firewallov obsahuje/zahŕňa špecializovaný aplikačný softvér a proxy service. *Proxy services* sú účelové programy, ktoré ovládajú komunikáciu cez firewall pre určité služby (HTTP alebo FTP). Sú špecifické pre protokoly navrhnuté na forward a poskytujú zvýšenú kontrolu prístupu, starostlivo detailnú kontrolu platnosti dát, generovanie audit záznamov o komunikácii a jej prenose. Každá aplikačná proxy vyžaduje dva komponenty, typicky implementované ako jednotlivo spustiteľné: proxy server a proxy client.



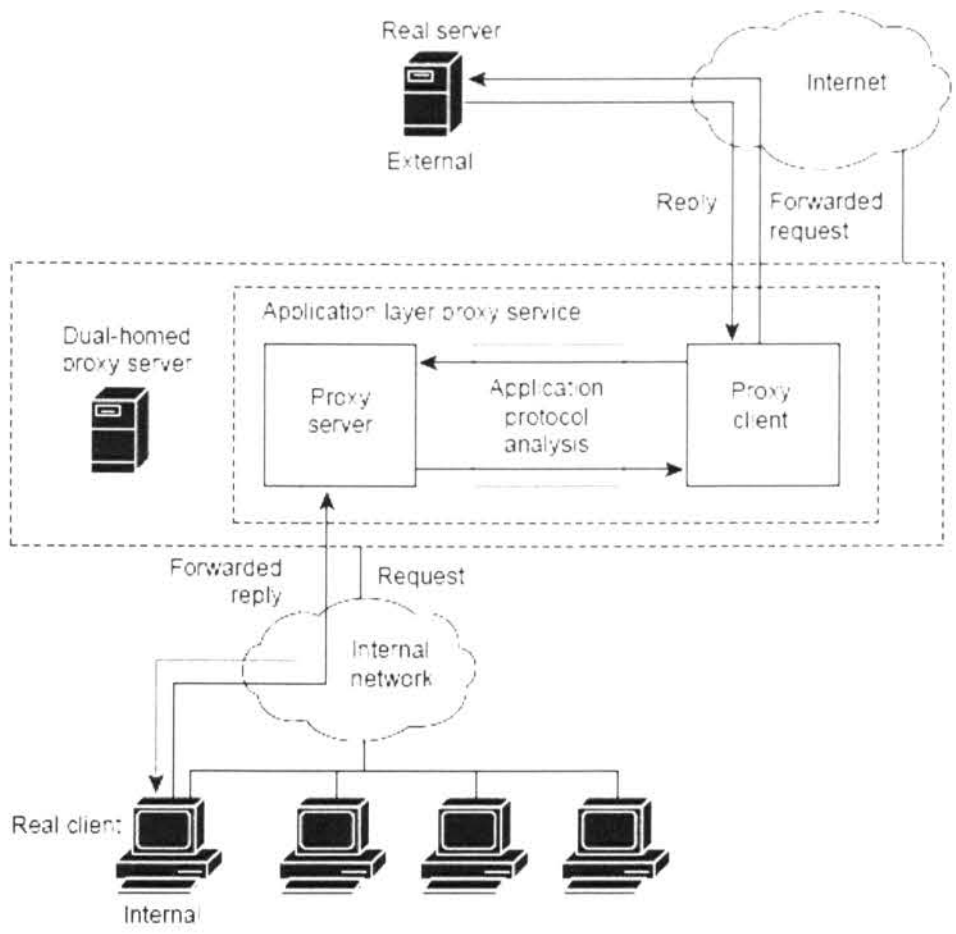
Obrázok 2.5: Ilúzia skutočnosti pri komunikácii cez proxy

Proxy server sa správa ako koncový server pre všetky požiadavky o spojenie vzniknuté v dôveryhodnej sieti skutočným klientom. Komunikácia medzi užívateľmi v sieti a Internetom prechádza cez proxy server, inak by museli užívatelia komunikovať priamo s ostatnými servermi na Internete. Proxy server vyhodnotí požiadavku prijatú od užívateľa a rozhodne, či ju povolí alebo zamietne na základe kolekcie pravidiel, ktoré sú nastavené individuálne pre sieťovú službu.

Ďalšími výhodami, ktoré proxy prináša, sú detailné audit záznamy informácií o session, užívateľská autentifikácia a zálohovanie.

Proxy client je časťou užívateľovej aplikácie a komunikuje s reálnym serverom v externej sieti v zastúpení skutočného klienta. Keď skutočný klient pošle žiadosť o službu, proxy server vyhodnotí požiadavku oproti pravidlám definovanými pre príslušnú proxy. Ak je povolená, proxy server postúpi požiadavku proxy klientovi, ktorý kontaktuje skutočný server. Proxy klient uskutočňuje prenos medzi proxy serverom a skutočným klientom.

Na obrázku 2.6 je zobrazený tok komunikácie medzi klientom a serverom s použitým proxy service.



Obrázok 2.6: Ako pracuje proxy service

Proxy service pracuje priehľadne medzi klientom a skutočným serverom a vytvára tak ilúziu, že z perspektívy užívateľa klient komunikuje priamo s reálnou službou na vzdialenom serveri. Naopak z perspektívy vzdialeného servera sa vytvára ilúzia, že server komunikuje s užívateľom na proxy serveri namiesto skutočného klientskeho počítača vo vnútri siete.

Služba ako proxy service je implementovaná na vrchole firewallového *protocol stack*u a pôsobí výhradne iba v aplikačnom priestore operačného systému. Preto každý paket musí prejsť najskôr nízko úrovňovými protokolmi postupujúc smerom hore cez protocol stack, aby mohli byť následne preskúmané hlavičky paketov a prenášané údaje práve proxy službou. Potom paket putuje naspäť do oblasti kernelu, smerom dole v protocol stacku, aby bol nasledovne distribuovaný ďalej. V rámci session je obdobne preskúmavaný každý paket, v dôsledku toho sú proxy služby pomalé.

Podobne ako stavové paketové firewally, aj tie aplikačné dokážu spĺňať dodatočnú kontrolu, či sieťové pakety neboli spoofnuté. S využitím princípu proxy service a *Network Address Translation* tak vnútorné IP adresy siete nemusia byť známe pre vonkajšie servery, zostávajú chránené pred priamym prístupom.

Medzi najvýznačnejšie nevýhody patria:

- Proxy service zapríčiňujú výkonové spomalenie. Prichádzajúce údaje sú spracovávané dvakrát, aplikáciou a jej príslušnou proxy. Napríklad Internetová e-mail aplikácia komunikuje s proxy e-mail agentom, ktorý striedavo komunikuje aj s LAN e-mail aplikáciou.

- Všeobecne nová proxy musí byť napísaná pre každý protokol, na ktorý má byť aplikovaná bezpečnostná politika firewallom. Rozšíriteľnosť je tak limitovaná.
- Aplikačné firewally nemôžu zabezpečovať proxy pre UDP, RPC a ďalšie z rodiny protokolov.
- Proxy services často vyžadujú modifikovanie klienta, čo predstavuje ďalšiu úlohu v konfiguračnom procese.
- Proxy services bývajú citlivé k operačnému systému a ku chybám na aplikačnej úrovni. Väčšina aplikačných firewallov potrebuje rozsiahlu podporu operačného systému na správne fungovanie, ktorá napríklad závisí na NDIS, TCP/IP, WinSock, Win32 alebo štandardných knižniciach jazyka C. Ak sa náhodou objaví bug (chyba) v niektorom z týchto komponentov, smie mať nežiaduci vplyv na bezpečnosť firewall servera.
- Proxy môže vyžadovať dodatočné heslá alebo iné validačné metódy, ktoré predstavujú oneskorenie a znižujú komfort užívateľa.

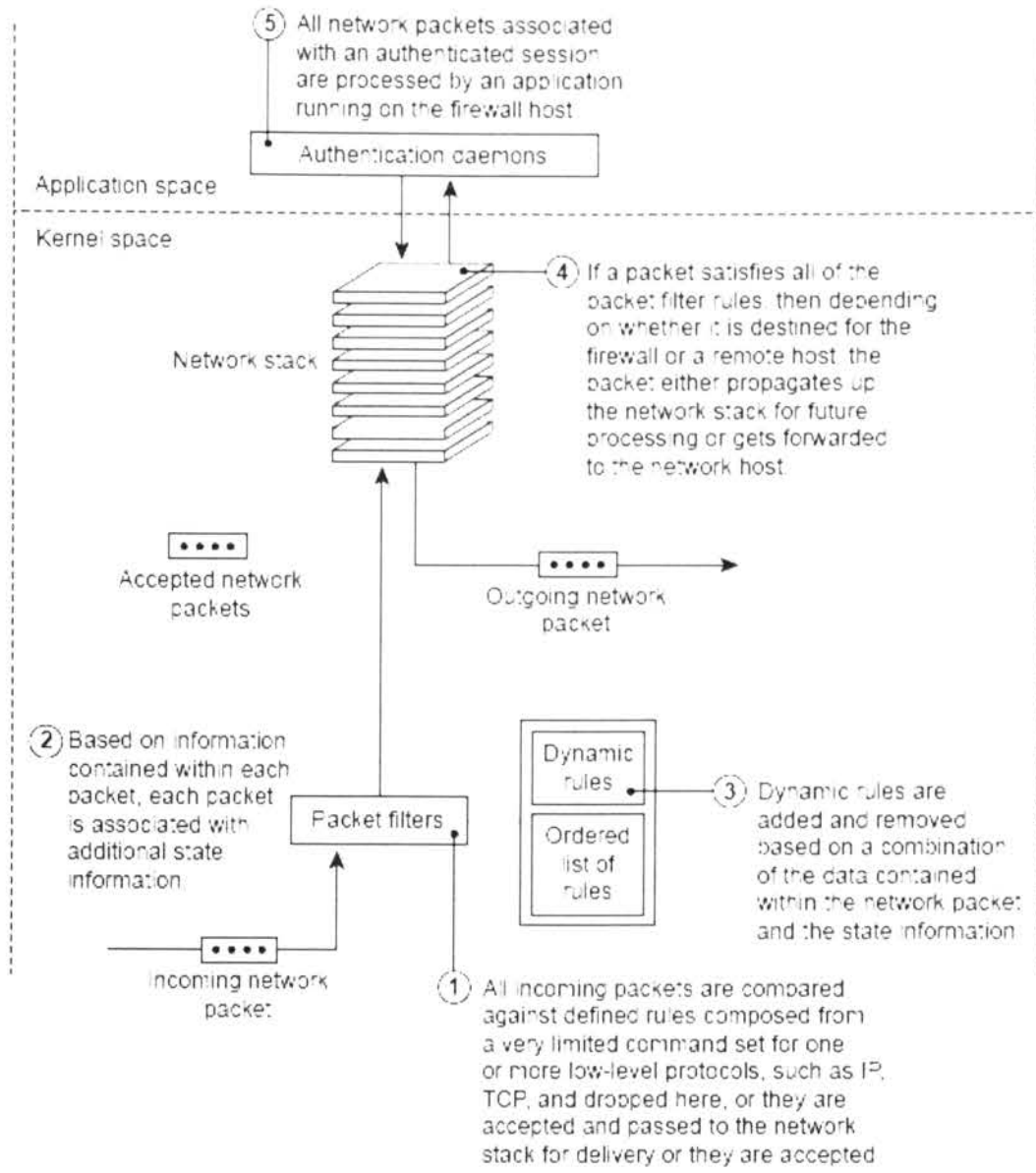
2.2.4 Dynamic Packet Filters

Dynamic Packet Filters, alebo *dynamické paketové filtre*, sú štvrtou generáciou technológie firewallov, ktoré povoľujú modifikáciu bezpečnostných pravidiel priebežne. Tento typ technológie je najvhodnejší v prípade limitovanej podpory transportného protokolu UDP, ktorý je typicky používaný vo forme žiadostí a odpovedí na výmenu informácií medzi protokolmi na vyššej, aplikačnej úrovni.

Firewall uskutočňuje funkčné požiadavky tak, že asociuje všetky UDP pakety k virtuálnym spojeniam, ktoré prelínajú bezpečnostné okruhy. Akonáhle je vygenerovaný paket s odpoveďou a zaslaný naspäť k pôvodnému žiadateľovi, v tom čase je vytvorené virtuálne spojenie a paket tak môže prejsť firewall serverom. Informácie o virtuálnom spojení sú zvyčajne uložené na krátky časový interval. Pri neprijatí paketu s odpoveďou počas intervalu, virtuálne spojenie sa stáva neplatným.

Na obrázku 2.7 je zobrazený proces vyhodnocovania sieťového paketu dynamickým paketovým filtrom.

Dynamické paketové filtre zdedili rovnaké výhody a nevýhody po prvej generácii firewallov - paketových filtrov. Avšak s jednou dôležitou výnimkou. Výhoda spočíva v zamietnutí nevyžiadaných UDP paketov. Po odoslaní požiadavky UDP paketom z vnútornej siete, firewall server presne definuje, čo musí byť obsiahnuté v prichádzajúcom pakete s odpoveďou aby bol doručený pôvodnej stanici. `Destination address` paketu musí odpovedať pôvodnej zdrojovej adrese, rovnako `destination port` transportnej vrstvy musí odpovedať pôvodnému zdrojovému portu, a musí súhlasiť typ transportného protokolu.



Obrázok 2.7: Dynamický paketový filter

Takáto charakteristika je prospešná pre aplikačné protokoly, akými je napríklad *Domain Name System*, ktorý pôsobí naprieč bezpečnostnými okruhmi. Vnútorný DNS server tak smie poslať dotaz o preloženie adresy na iné DNS servery bežiace na Internete využívajúc buď TCP spojenie alebo UDP virtuálne spojenie.[1]

Ďalšou významnou otázkou je dátový kanál používaný protokolom FTP, ktorý je nemožné transparentne ovládať bez akejkoľvek špecifickej aplikačnej znalosti. So spojením na port 21[5] firewall typicky špeciálne zaobchádza. Tok príkazov je prehľadávaný, lebo hodnoty príkazov `PORT`[6] sú použité na aktualizovanie filtrovacej tabuľky. Dátové spojenie pri aktívnom režime FTP je iniciované klientom.

Skenovanie môže byť uskutočnené aj v pasívnom móde pri `PASV` príkaze[7], treba však nastaviť filtrovanie odchádzajúcich spojení. Dátové spojenie je iniciované klientom, lebo firewally neakceptujú žiadosť o otvorenie spojenia vedúceho dovnútra na náhodný port.[4]

[5] port FTP riadiaceho kanálu, na ktorom server načúva

[6] príkaz zasielaní v aktívnom móde klietom v tvare `PORT 192,168,0,1,192,2`. To znamená, že server pošle klientovi dáta na IP 192.168.0.1 a na port 192x256 + 2 = 49154.

[7] príkaz zasielaní v pasívnom mode klientom, syntax rovnaká ako u príkazu `PORT`. IP adresa určuje, kam má server smerovať odpoveď.

2.3 Výkon vs. bezpečnosť

Pri zvažovaní alternatívnych firewall technológií sa naskytne otázka: "Aký kompromis zvoliť medzi výkonom a bezpečnosťou?" Pri odpovedi na túto otázku treba vziať do úvahy ako vysoko v *protocol stack*u sa musia dostať sieťové pakety. Paketové filtre všeobecne dosahujú najvyšší výkon, nasledujúc stavovými paketovými firewallmi, dynamickými paketovými filtrami a aplikačnými firewallmi.

Úroveň bezpečnosti a jej kontroly vyjadruje zoznam technológií firewallov presne v opačnom poradí, pretože ako sieťové pakety prechádzajú viac protokolových vrstiev tak sú kontrolované detailnejšie. Za najbezpečnejšie sú považované aplikačné filtre.

Paradoxom je, že stavový paketový filter, ktorý nevykonáva rozsiahlejšiu bezpečnostnú kontrolu ako len priraďovanie paketu k platnému spojeniu, je rýchlejší ako paketový filter, ktorý obsahuje početný zoznam `accept` a `deny` pravidiel.

Všeobecne sú aplikačné firewally považované za najpomalšie v dôsledku, že všetky pakety sú predávané smerom ku vyšším vrstvám jedným *network stack*om a spätne smerom dole iným. Výsledne sa tak zaobchádza ako s dvoma samostatnými sieťovými reláciami (network sessions).

2.4 Čo firewally nedokážu

Hoci sú firewally užitočnou súčasťou sieťovej bezpečnosti, nie sú všeliek. Keď sú nastavené správne, sú prospešné, ale nedokážu všetko. Ak sú používané nesprávne, jediným ich prínosom je falošný pocit bezpečnosti.

Firewally sú bezmocné proti útokom z vnútra. Útok z vnútra môže byť od niekoho, kto prešiel k "temnej strane", alebo od niekoho, kto získal prístup do vnútornej siete inými prostriedkami.

Ak je firewall jediným bezpečnostným mechanizmom a niekto sa dostane do siete nejakým iným mechanizmom - máme problém. Ak sa uskutočňuje vírusové skenovanie e-mailov iba na vstupnej bráne, bezpečnosť môže byť prerušená z vnútra napríklad infikovaným USB flash diskom alebo stiahnutým spustiteľným súborom z Webu.

Firewall pracuje na nejakej vrstve *protocol stack*u. Čo znamená, že sa nepozerá na nič vo vyšších vrstvách. Ak prebieha filtrovanie podľa čísel portov na transportnej vrstve, unikajú problémy so SMTP. Ak filtrujeme SMTP, unikajú data-driven[8] problémy v hlavičkách mailov. Ak sú prezerané hlavičky mailov, unikajú vírusy a Trójske kone.[1] Je dôležité ohodnotiť riziká hrozieb na každej vrstve. Filtrovanie vo vyšších vrstvách je viac dotieravé, pomalšie na spracovanie a menej jednotné. Postupovaním nahor v protocol stacku sa vytvára oveľa viac možností na spracovanie každého paketu.

[8] architektúra/jazyk, riadený pomocou dát, vykonáva výpočty v poradí určenom závislosťami dát

Skenovanie proti e-mail vírusom je dominantou windowsovských sietí. Zahadzovanie e-mailov obsahujúcich vírus na vstupnej bráne môže dokonca ušetriť prenosovú kapacitu. Dobrou stratégiou je mať jeden druh vírusového skenera na vstupnej bráne (Gateway) a ďalší na koncových počítačoch. Naopak skenovanie FTP sťahovaní nie je užitočné vo väčšine sietí. Transformovanie dát (napr. kompresia) robí úlohu virtuálne nemožnou, obzvlášť pri rýchlosti linky.

Ďalším problémom firewallov je tranzitivita dôvery. Treba s ňou počítať. Ak A verí B, B verí C, tak potom A verí C či chce alebo nie.

Firewally môžu obsahovať chyby alebo nepracovať ako sa očakáva. Aj najlepšia administrácia nezmôže nič, ak firewall nefunguje ako sa uvádza v dokumentácii.

2.5 Z pohľadu užívateľa

Personal Firewall

Personall firewall, alebo osobný firewall, je aplikácia, ktorá kontroluje prichádzajúce aj odchádzajúce sieťové spojenie počítača. Na základe pravidiel bezpečnostnej politiky (security policy) povoľuje alebo zamieta jednotlivé komunikačné spojenia.

Osobný firewall je typicky navrhnutý pre koncového užívateľa. Zvyčajne chráni iba počítač, na ktorom je inštalovaný. Môže poskytovať aj určitú úroveň hĺbkovej detekcie. V prípade podozrenia o pokus vniknutia do systému, ponecháva softwaru možnosť prerušiť alebo blokovať spojenie.

Hlavné črty osobného firewalu:

- upozornenie užívateľa o pokuse o odchádzajúce spojenie
- dovoliť užívateľovi kontrolovať ktoré programy sa môžu/nemôžu pripojiť k lokálnej sieti alebo Internetu
- skryť počítač pred skenovaním portov neodpovedajúc na nevyžiadané sieťové spojenie
- monitorovať aplikácie, ktoré čakajú na prichádzajúce spojenie
- monitorovať a regulovať všetky prichádzajúce a odchádzajúce internetové spojenia
- zabrániť/predísť nechceným sieťovým spojeniam od lokálne inštalovaných aplikácii
- poskytovať užívateľovi informácie o aplikáciách, ktoré sa pokúšajú o spojenie
- poskytovať informácie o cieľovom servere, s ktorým sa aplikácia chystá nadviazať spojenie

Veľké množstvo vygenerovaných upozornení aplikáciami môže viesť k zníženiu citlivosti užívateľa rozoznať skutočné hrozby od menej záľudných (napr. ICMP request). Ak je systém vybavený softwarom *Malware*, *Spyware* alebo iným, tieto programy môžu zmanipulovať firewall, pretože oba bežia na rovnakom systéme. Do úvahy prichádza obídenie alebo dokonca úplne odstavenie firewallu.[16]

Distributed Firewalls

Najnovšou formou firewallov, ktorá ešte nie je dostupná v plnej nádhere, sú *distribuované firewally*. Každý samostatný hostiteľský počítač uplatňuje bezpečnostnú politiku, ktorá sama je nastavená centrálnym riadiacim uzlom. Pravidlo na zamietnutie určitého pokusu o spojenie je vytvorené administrátorom a poslané každému hostiteľskému počítaču v spravovanej doméne. Výhodou tejto schémy je schopnosť chrániť zariadenia, ktoré nie sú v topologicky izolovanom priestore. Množstvo komerčných produktov sa správa približne podobne, ale je ľahké si to prispôsobiť kombináciou špecifikácie vysoko úrovňovej bezpečnostnej politiky s nejakým druhom súborového distribučného mechanizmu (Server Management System od Microsoftu).[1]

2.6 Z pohľadu architektúry siete [12]

V tejto sekcii uvediem a popíšem rôzne spôsoby zapojenia komponent firewallu do siete. V čom spočívajú výhody a nevýhody príslušných architektúr siete.

Single-box architektúry

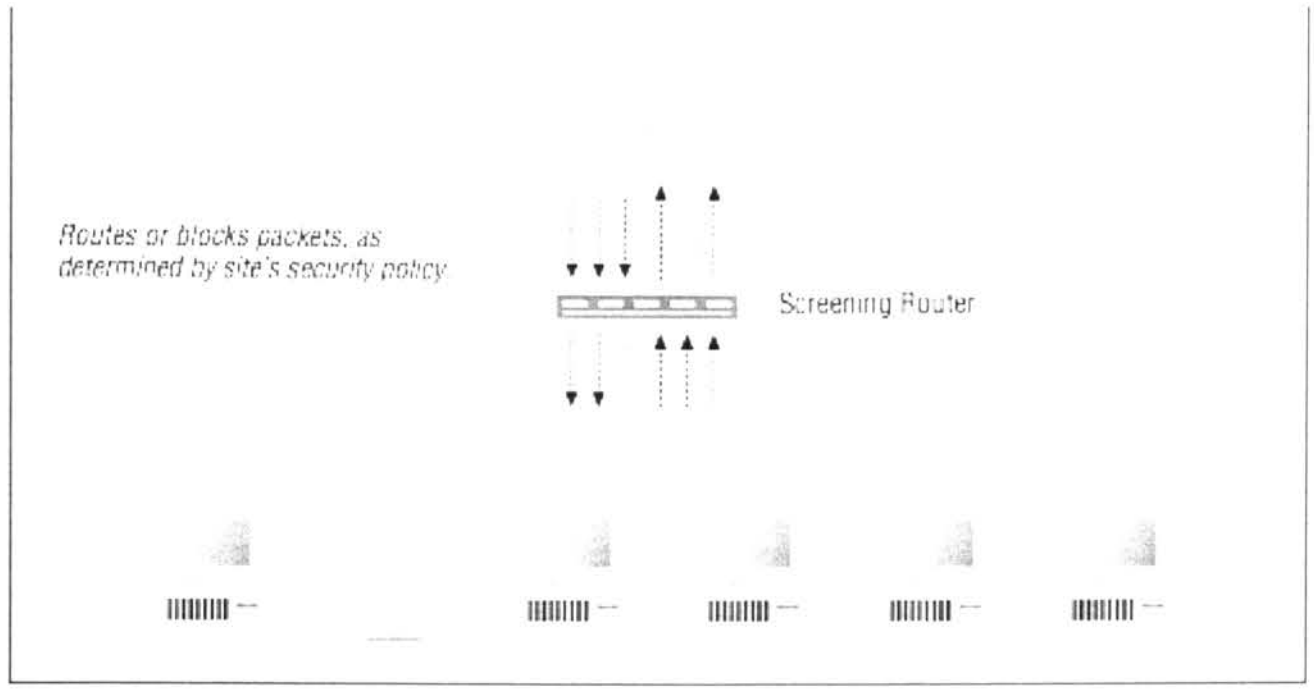
Najjednoduchšia firewallová architektúra siete má iba jeden objekt, ktorý pracuje ako firewall. Všeobecne výhoda *single-box* architektúry spočíva v tom, že predstavuje jediné miesto, ktoré vyžaduje koncentráciu administrátora a spoľahlivo správnu konfiguráciu. Zároveň nevýhodu je, že bezpečnosť úplne závisí od tohto miesta.

Výhody *single-box* architektúr v praxi nezávisia od zabezpečenia ale od iných praktických súvislostí. V porovnaní s viac vrstvovými systémami integrovanými do siete, sú lacnejšie, ľahšie na pochopenie a vysvetlenie pre správu a jednoduchšie si ich priamo obstarať od externého dodávateľa. Predstavujú riešenie pre malé siete.

2.6.1 Screening router

Možným riešením single-box architektúry je použitie samotného paketového filtrovacieho systému ako firewall. *Router*, alebo *smerovač*, tak chráni komplentne celú sieť. Predstavuje finančne nenáročné riešenie, a v takmer každom prípade je router nevyhnutný aj na pripojenie do Internetu.

Router, ako príslúšný firewall, býva využívaný v situacií, keď stanice v sieti sú dostatočne zabezpečené na vyššej úrovni, počet povolených protokolov je limitovaný,

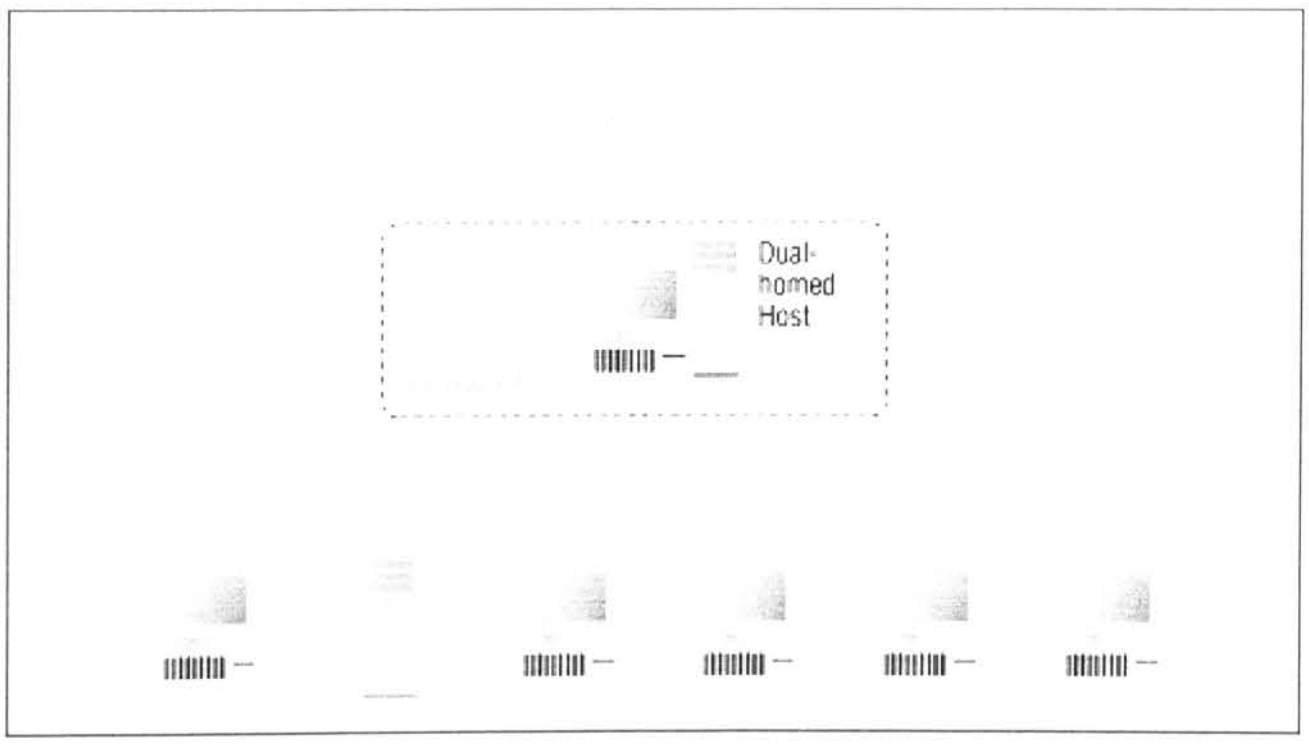


Obrázok 2.8: Preverovací smerovač

protokoly komunikujú priamočiaro (bez proxy), alebo keď ochraňovaná sieť je vyhradená na poskytovanie služieb na Internete. T.j. sú v nej umiestnené public servery určené na komunikáciu so svetom.

2.6.2 Dual-Homed Host

Dual-homed host architektúra je postavená na dual-homed počítači, ktorý má aspoň dve sieťové rozhrania. Takýto počítač by sa mohol správať podobne ako router medzi dvomi sieťami, ktoré sú naň pripojené. Avšak pakety nie sú smerované priamo z vonkajšej siete (Internet, unknown network) do vnútornej siete (internal, trusted network). IP traffic medzi nimi je blokovaný. Sieťová architektúra s použitím dual-homed host firewallom je zobrazená na obrázku 2.9.



Obrázok 2.9: Dual-homed host architektúra

Ak nie sú vôbec povolené pakety medzi vonkajšou a vnútornou sieťou, objavenie paketov s vonkajšou zdrojou adresou vo vnútornej sieti indikuje určitý bezpečnostný problém.

Dual-homed firewally v porovnaní s paketovými filtrami sú menej výkonné, nedokážu zabezpečiť komunikáciu v takom objeme ako ekvivaletné paketové filtrujúce systémy. Daľšou neýhodou je, že predstavujú jediný bod zlyhania. V prípade zneužitia tejto stanice, môže útočník získať plný prístup k vnútornej sieti, odpojiť pripojenie k Internetu, a tak zabrániť podnikaniu spoločnosti a výmene informácií s klientom.

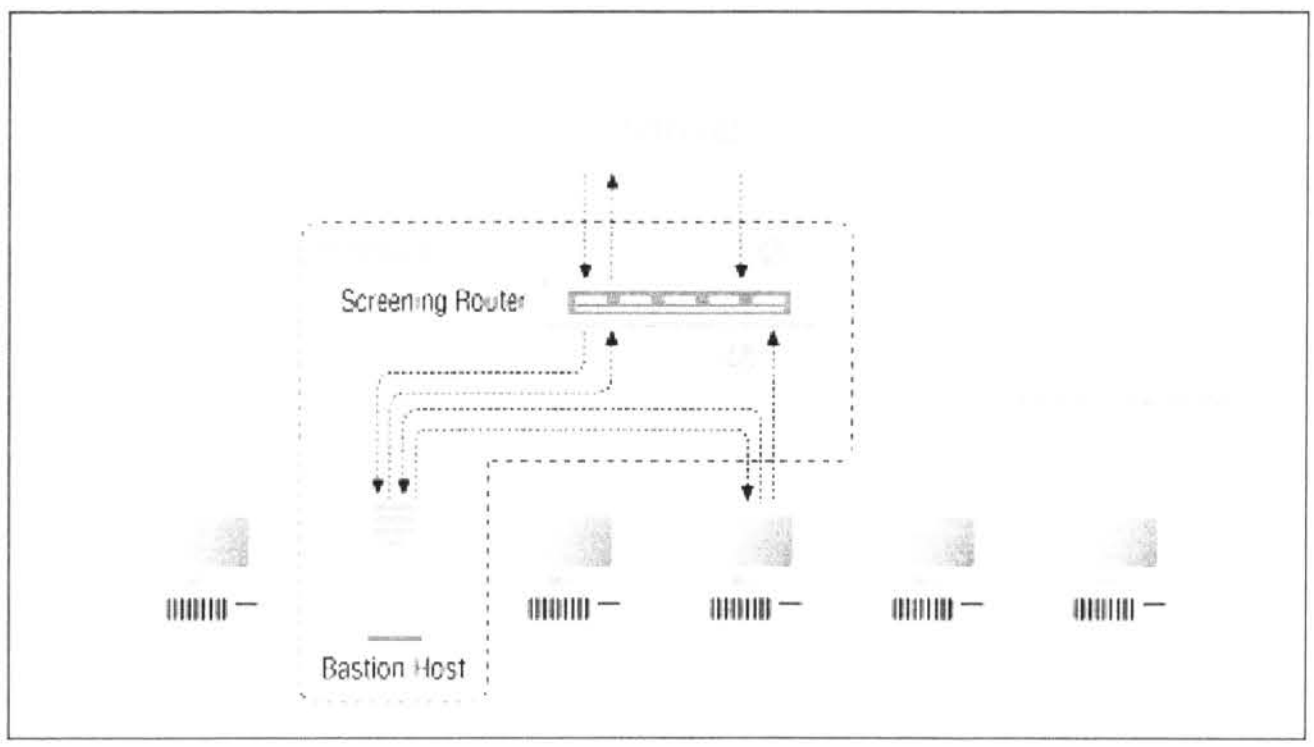
Dual-homed počítač môže poskytovať služby iba vo forme proxy, prípadne povoliť užívateľovi sa prihlásiť na tento počítač. Užívateľské kontá predstavujú riziko zneužitia - môže dôjsť k zlyhaniu ľudského faktoru tým, že prihlásený užívateľ nečakane povolí službu považovanú za nespoľahlivú. Samotný proces autentifikácie na túto stanicu je pre užívateľov nepohodlný.

Dual-homed host je vhodné používať, ak objem komunikácie s vonkajšími sieťami (Internetom) je pomerne malý, a nie je rohodujúci pre obchodný model spoločnosti, alebo ak vnútorné stanice siete neobsahujú citlivé údaje.

2.6.3 Screened Host Architecture

Screened host architektúra poskytuje služby len pre stanice, ktoré sú pripojené k vnútornej sieti s použitím samostatného smerovača. Primárna bezpečnosť siete je zaistená paketovým filtrovaním na smerovači, ktoré zabraňuje užívateľom obchádzať proxy server a vytvárať priame spojenia, ako to bolo možné u dual-homed host architektúre.

Na obrázku 2.10 je zobrazená jednoduchá verzia screened host architektúry. Filtrovanie je nastavené tak, aby bastion host bol jediným systémom, na ktorý je možné sa pripojiť z Internetu (napríklad doručovanie e-mailov). Naopak aj bastion host má povolené odchádzajúce spojenia.



Obrázok 2.10: Preverovacia stanica

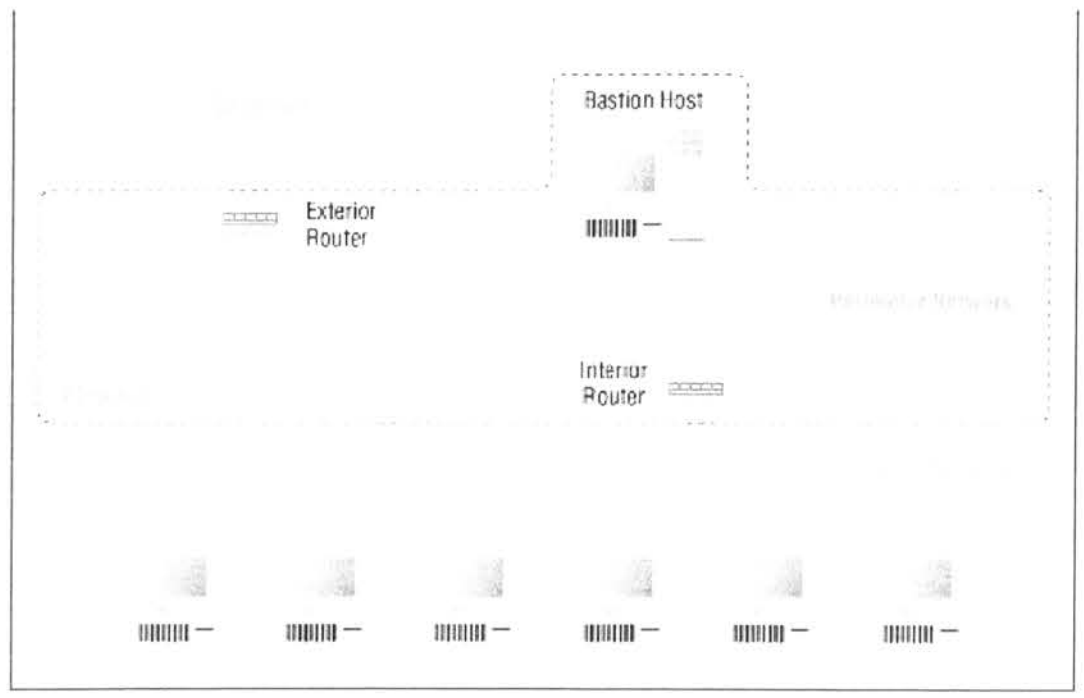
Optimálne nastavenie reprezentuje kombinácia dvoch prístupov, povolenie niektorých služieb priamo cez paketové filtrovanie, zatiaľ čo iné služby komunikujú len pro-

stredníctvom proxy. V porovnaní s dual-homed host poskytuje táto architektúra lepšiu bezpečnosť a širšiu použiteľnosť. Je menej náročné chrániť smerovač ako aplikačnú bránu.

Nevýhodou tejto architektúry je, že smerovač predstavuje jediný bod zlyhania. Rovnako po zdarenom zneužití aplikačnej brány umiestnenej na *bastion host* už nič nestojí v ceste sieťovej bezpečnosti medzi bastion host a zvyškom vnútornej siete. Taktiež nie je vhodné zriadiť rizikové služby ako web server na bastion host, ktorá je pripojená priamo do vnútornej siete.

2.6.4 Screened Subnet Architecture

Screened subnet architektúra pridáva extra vrstvu zabezpečenia siete. Vzniká doplnením *perimeter siete* ku *screened host* architektúre, a tak izoluje internú sieť od Internetu. S vytvorením subnetu sú do architektúry zapojené dva smerovače, jeden medzi perimeter network a vnútornú sieť, a druhý medzi perimeter network a vonkajšiu sieť. Na preniknutie k vnútornej sieti, musí útočník prejsť cez oba smerovače. V prípade preniknutia do aplikačnej brány (bastion host), stále sieť chráni vnútorný smerovač.



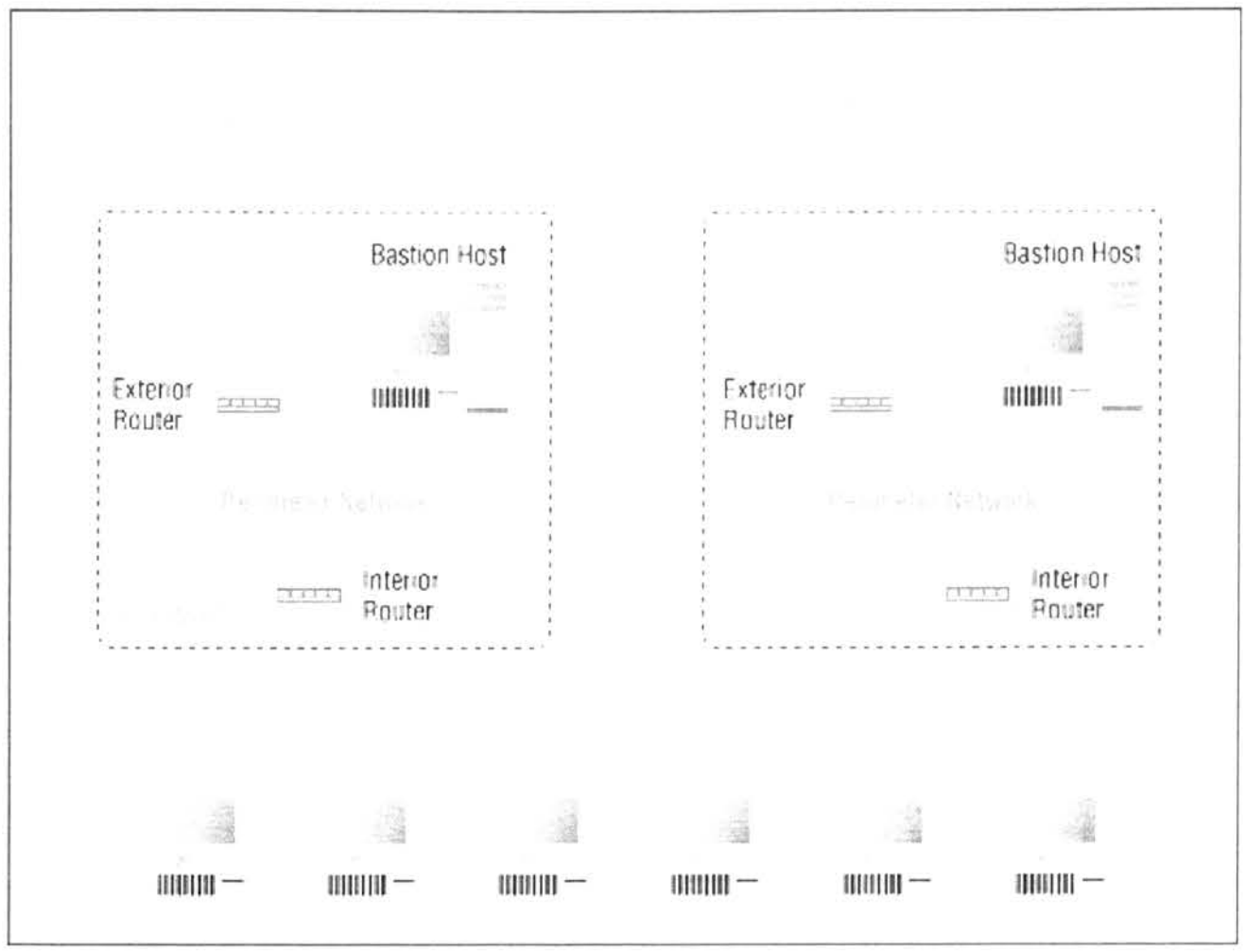
Obrázok 2.11: Preverovaný subnet

Na obrázku 2.11 je zobrazená možná firewall konfigurácia, ktorá používa screened subnet architektúru.

Independent Screened Subnets

V niektorých prípadoch je žiadúce mať viaceré, *nezávislé subnety - independent screened subnets*, so samostatnými externými routerami. Architektúra s použitím viacerých perimeter networks je zobrazená na obrázku 2.12.

Táto architektúra sa dá docieliť vytvorením dvoch *perimeter networks*, zriadením dvoch pripojení do Internetu, dvoch externých a dvoch interných smerovačov. Získaná redundancia sa na jednej strane javí ako predražená a zbytočná, ale na druhej strane nie



Obrázok 2.12: Paralelné okrajové siete

je rizikom zlyhania jediný bod medzi vnútornou sieťou a Internetom. Viaceré nezávislé subnety zabezpečujú privátnosť, ak je jeden využívaný na prenos dôverných údajov a iný na pripojenie do Internetu.

Výhodou takejto konfigurácie siete je možnosť na oddelenie prichádzajúcich spojení a služieb poskytovaných pre vonkajších klientov (verejne prístupné web servery) od odchádzajúcich spojení a služieb (web cache proxy službu).

3 Filtrovanie služieb

Rozhodnutie, aké služby filtrovať paketovými filtrami a firewallmi, záleží od požadovanej bezpečnostnej politiky. Napokon niektoré všeobecné filtrujúce pravidlá je rozumné aplikovať pre väčšinu politík. Táto kapitola rozoberá *čo* filtrovať a *prečo*. Je zameraná na najviac zaujímavé služby.

Na opísanie a zhrnutie, ako zaobchádzať so službami z bezpečnostného hľadiska, si pomôžem nasledujúcou tabuľkou:

protocol	**out**	**in**	**comment**
PROTOKOL	x	y	*komentár*

V tabuľke možu x a y nadobúdať hodnoty:

allow nechať prejsť /prepustiť
block nenechať prejsť /neprepustiť
filter proxy na aplikačnej úrovni rozhodne
tunnel blokovať port PROTOKOLu, ale povoliť užívateľom vytvoriť tunel pomocou bezpečnejšieho protokolu

Stĺpec *out* odkazuje na rozhodnutie o odchádzajúcom (outbound) spojení pre port PROTOKOLu. Pre TCP pakety je odchádzajúce spojenie priame, iniciované z vnútra. Prichádzajúce (inbound) je naopak iniciované z vonku.

Odlišný význam je pre protokol UDP, pretože je bezspojový. Okrem toho, nie všetky protokoly sú jednoducho query/response službami. Pre query/response služby môžeme hovoriť o "inbound query" (prichádzajúca požiadavka), ktorá vyvolá "outbound response" (odchádzajúca odpoveď). Podobne "outbound query" vyvolá "inbound response". Pre protokoly nezapadajúce do tohto modelu môžeme hovoriť iba o prichádzajúcich a odchádzajúcich paketoch (napr. TCP).

3.1 Služby rozumné filtrovať [1]

DNS

DNS predstavuje dilemu pre sieťových administrátorov. Potrebujeme informácie z vonku a pritom nedôverujeme name-to-IP mapovaniu z vonku. Presnejšie, absolútne nesmieme dôverovať takýmto informáciám pre vnútorné účely. Hoci možno byť od nich závislý, napríklad v prípade posielania e-mailu vonkajším spolupracovníkom.

Toto má aj následky. Hoci za určitých okolností môže byť v poriadku name-based autentifikácia pre interné počítače, ale nikdy nie je akceptovateľná pre externé. Musíme zaistiť, aby žiadny dôveryhodný vzťah internal-to-internal (vzťah vnútornej komunikácie) nezávisel od informácie poskytnutej z vonku.

Hrozba je jednoduchá: útočník môže kontaminovať DNS cache do značnej miery priložením cudzej informácie k vyžiadanej odpovedi (response). Pravidlá pre odchádzajúce DNS požiadavky môžeme sumarizovať ako:

protocol	outbound query	inbound response	comment
DNS	allow	filter	*Blokovať interné informácie*

Najlepším spôsobom ako filtrovať DNS je použitie DNS proxy, ktorý prináša dve výhody:

- Presmerovanie požiadaviek o interných informáciách na vnútorný DNS server. Požiadavka tak nebude nikdy priamo odoslaná na vonkajšie servery.
- Cenzurovanie prichádzajúcich odpovedí na zaistenie, aby nevracali zdanlivo interné informácie. To sa môže objaviť v odpovedi zmenou sekcií *Aditional Information* alebo *Authoritative Server*.

Prichádzajúce požiadavky (queries) sa dajú riešiť jednoduchšie, a to umiestnením DNS servera do DMZ. Záležitosťou operatívnej správnosti je mať aspoň dva DNS servery pre každú zónu. A zaistiť, aby boli od seba v separovaných častiach Internetu a už vôbec nie v tej istej LAN. Z bezpečnostného hľadiska tak sťažiť útoky typu DDoS (Distributed denial of service - zahltenie servera požiadavkami).

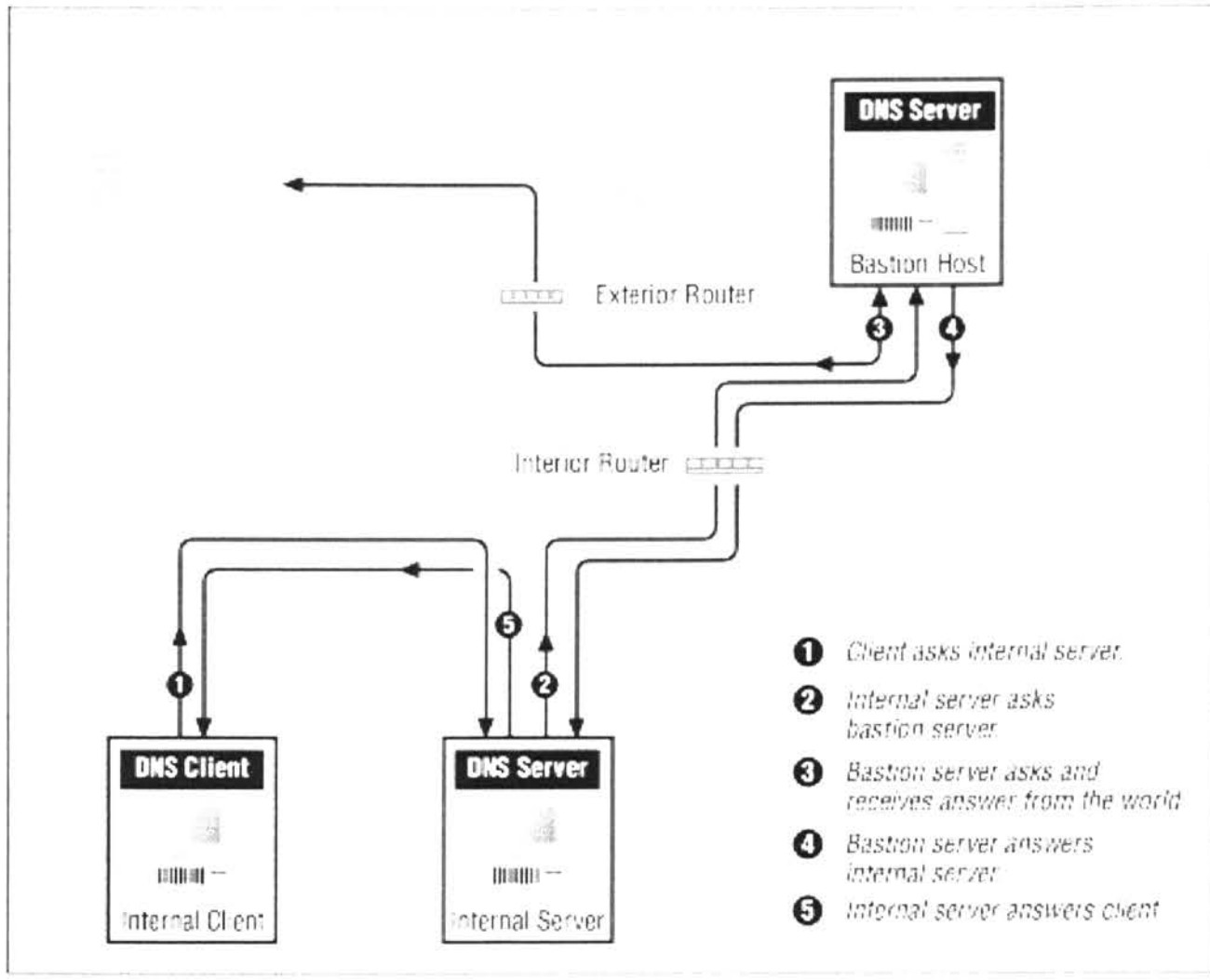
protocol	outbound response	inbound query	comment
DNS	allow	DMZ	

Pojednávanie s DNS je jedným z najzložitejších problémov nastavenia firewallu, obzvlášť pri použití jednoduchého paketového filtra. Ak beží circiut alebo application gateway, netreba používať vonkajší DNS vnútorne. Informácie poskytované vonkajšiemu svetu môžu byť minimálne. Dynamické paketové filtre dokážu zachádzať na jednej úrovni s DNS tak dôkladne ako s každým iným UDP založeným protokolom.

Vnútorné počítače potrebujú používať DNS na dosiahnutie vonkajších sietí. Chapmanovo priblíženie[10] spočíva v spustení *name servers* pre doménu na gateway počítači a nejakom vnútornom. NS na vnútornom počítači má skutočnú informáciu, pokiaľ gateway names server má akýsi minimálny popis zóny.

Problémové miesta sú:

- Povoliť pre Gateway preklad interných názvov/mien (napríklad pre doručenie mailu).
- Povoliť pre vnútorné počítače preklad externých názvov/mien.
- Poskytnúť spôsob pre nevyhnutné UDP pakety ako prekročiť firewall.



Obrázok 3.1: DNS forwarding s použitým dvoch DNS serverov

Prvý problém jednoducho zvládnuť vytvorením súboru `/etc/resolv.conf` na gatewayi (Bastion Host na obrázku 3.1), ktorý odkazuje na vnútorný DNS server (Internal Server na obrázku 3.1). Tento súbor povie aplikačným programom bežiacim na gatewayi, ale nie DNS samotný, kam ísť s prekladom požiadaviek. Napríklad kedykoľvek *mail* chce nájsť IP adresu, opýta sa vnútorného serveru.

Name server proces nevenuje pozornosť súboru `/etc/resolv.conf`. Jednoducho používa stromovú štruktúru menného priestoru (tree-structured namespace) a znalosti root name serveru na spracovanie všetkých požiadaviek.

Druhý problém zahŕňa požiadavky na vonkajšie mená poslané na vnútorný name server. Samozrejme že server o vonkajších počítačoch nič nevie. Namiesto priamej komunikácie so skutočnými serverami (nemožno povoliť priamo, nedostali by sme odpovede cez firewall), vnútorný server má `forwarder` záznam v konfiguračnom súbore smerujúci na gateway. Tento záznam označuje, ktorý server by mal byť dotazovaný na mená, ktoré nie sú známe lokálne. Teda ak sa pýtame na vnútorné mená, odpovedá priamo, ak sa pýtame na vonkajšie mená, posúva požiadavku na gateway name server.

Kuriózna cesta nastáva pri požiadavke na preklad o vonkajšie mená spracovávanej na gatewayi. Najskôr putuje na vnútorný server, ktorý odpoveď nepozná pokiaľ nemá cache. Potom preskočí spať cez firewall na vonkajší server na gatewayi, a odtiaľ až smeruje na vzdialený DNS server, ktorý pozná odpoveď. Odpoveď cestuje tou istou kľukatou cestou.

Dôvod prečo vnútorný a vonkajší name server komunikujú cez paketový filter (Inte-

rior router s úlohou filtrovania na obrázku 3.1) je, že DNS servery používajú nemenné číslo portu pri posielaní ich požiadaviek. Toto rieši tretí problém.

Web

Firewall by nemal povoľovať prichádzajúcu premávku, s výnimkou prístupu k oficiálnemu Web serveru. Samozrejme ten by mal byť umiestnený v DMZ. Pakety smerujúce na port 80 na vnútorné počítače by mali byť zamietnuté. Dosť z týchto paketov býva generovaných automaticky červami hľadajúc nové ciele.

protocol	out	in	comment
Web	allow	block	*Umiestniť Web server do DMZ*

V alternatívnom prípade nepovoliť odchádzajúci traffic úplne, ale ho filtrovať, ak sa vyžaduje aby užívatelia siete komunikovali so svetom iba cez vnútornú Web proxy.

FTP

FTP môže byť zradný protokol. Pretože štandardne FTP používa `PORT mode`, ktorý vyžaduje samostatné prichádzajúce spojenie. Mnoho stavových (STATEFUL) firewallov tak otvára dieru pre prichádzajúce spojenia na vnútorné počítače. Lepším riešením je požadovať využívanie `PASV` príkazu FTP pre odchádzajúce spojenie. Aj tak veľa browserov beží v pasívnom móde, hoci niektoré požadujú nastavenie. Pravidlá sú teda nasledujúce:

protocol	out	in	comment
FTP	passive	block	*Umiestniť FTP server do DMZ*

TCP

Je dobrou myšlienkou povoliť prichádzajúce a odchádzajúce TCP spojenie? Hlavným pravidlom je dôverovať interným pracovníkom - užívateľom. Ak im nemožno dôverovať, nastáva problém zlyhania ľudského faktoru, ktorý býva obvykle oveľa závažnejší ako sieťový problém.

> *"Technology can't solve social problem."*
>
> Ranum's Law

Hoci môžeme dôverovať vnútorným užívateľom siete, nie vždy však spúšťajú kód, ktorý sa chová správne. Napríklad podpísané applety bežiace na vnútorných počítačoch. Appletu môže prideliť práva naivný užívateľ, a potom tak smie komunikovať s file systémom a pripájať sa ľubovoľné miesta na sieti. TCP spojenie vznikajúce pomocou appletov pochádza z vnútra.

Existujú ďalšie spôsoby ako iniciovať problematické odchádzajúce spojenie. Predpoklad, že e-mail je filtrovaný od vírusov a červov, platí pri získavaní e-mailu cez POP3

alebo IMAP. V prípade, že e-mail je čítaní cez Web-based server ako Hotmail, ťažko zabrániť infikovaniu. Filtrovanie takýchto mailov nespadá pod bezpečnostnú politiku spoločnosti aplikovanú na elektronickú poštu.

Zamietnutie všetkých odchádzajúcich spojení predstavuje obmedzenie, ktoré je pravdepodobne až príliš silné. Naopak, vysoko citlivé vládne siete ospravedlňujú takúto politiku požiadavkami na diskrétnosť a utajenie ich dát.

Prichádzajúce TCP spojenie by nemalo byť povolené. Prístup z vonku je tak ovládaný cez príslušnú proxy, často umiestnenú v DMZ. Prístup môže byť riešený kryptograficky zdokonalenými službami, ako *ssh*.

protocol	**out**	**in**	**comment**
TCP	allow	block	*Všeobecne dôverovať interným užívateľom*

NTP (Network Time Protocol)

V súčasnosti sú dostupné lacné, extrémne presné časové zariadenia založené na pricípe GPS a iných rádiových zdrojov. Alebo sa dajú použiť rozličné zdroje presného času na Internete. Je vhodné limitovať prístup iba na zvolené/vybrané externé servery.

protocol	**out**	**in**	**comment**
NTP	allow	allow	*Iba určité hostiteľské servery*

Ďalšou možnosťou je vytvoriť vlastný externý NTP server a cez firewall povoliť pre vnútorné počítače spojenie s ním.

SMTP/Mail

V prípade elektronickej pošty je vhodné kontrolovať e-mail na vírusy, neobvyklé prílohy, alebo dokonca na korporačné tajomstvá a neslušné slová. V extrémnych prípadoch je potrebné zasiahnuť odstránením. Rozpoznávanie slov a fráz sa stretáva s problémom rozpoznávania prirodzeného jazyka.

ISP, ako poskytovateľ Internetu, má ďalší dôvod na blokovanie odchádzajúcej SMTP služby, ak spameri nájdu otvorené servery *open relays*[1], a začnú rozosielať maily s fiktívnymi hlavičkami a zahlcovať nimi e-mailové schránky. Blokovanie je rozumná politika pre služby, ktoré majú nezodpovedných spotrebiteľov.

Ak žiadny zo sporných bodov nie je dôležitý, odchádzajúce spojenie môže byť povolené a bez filtrovania.

protocol	**out**	**in**	**comment**
SMTP	allow	filter	

[1]je SMTP server konfigurovaný spôsobom, že povoľuje hocikomu na Internet poslať cez neho e-mail, nie nutne smerovaný pre známych, alebo zaslaný od známych užívateľov. Veľa takýchto serverov bolo uzavretých alebo umiestnených na blacklist ostatnými serverami.

POP3/IMAP

Prichádzajúce POP3 a IMAP spojenie sa pokúša pripájať do siete za účelom získať alebo doručiť e-mail. Je takmer isté, že citlivý vnútorný obsah elektronickej pošty by nemal byť vystavený zvedavým očiam, preto POP3 poskytuje viaceré autentifikačné metódy proti neoprávnenému prístupu. Jednou z nich je APOP protokol využívajúc *challenge/response login*[2], ktorý je napadnuteľný útokom typu *dictionary attack*[3]. Poskytovať prístup pre tieto protokoly sa dá pomocou tunela. Väčšina mailových klientov a serverov podporuje tieto protokoly cez SSL.

Pri odchádzajúcom spojení a prístupe na POP3/IMAP servery nastáva problém s vystavením hesla a tiež so zlomyseľným obsahom e-mailu (prílohy). Požiadavky na externé servery cez proxy na aplikačnej úrovni možno skenovať na vírusy, červy a ďalšie spustiteľné súbory, poprípade pridať spam filter.

protocol	out	in	comment
POP3/IMAP	filter	block	*Blokovať aktívny obsah*

ssh

Ssh je rozumné povoliť cez firewall, pretože implementuje kryptografickú autentifikáciu a šifrovanie. A býva najlepším spôsobom ako povoliť prístup cez firewall.

protocol	out	in	comment
ssh	allow	allow	

Možno sa zdá byť výhodné ukončiť všetky prichádzajúce ssh spojenia na úrovni firewallu, a vytvoriť silný centralizovaný autentifikačný mechanizmus. Ak je odchádzajúce TCP spojenie povolené, je jednoduché vytvoriť zadné dvere s použitým *ssh port-forwarding*.

3.2 Problémové služby [1]

UDP

Filtrovanie UDP paketov a stále udržanie kompletnej funkčnosti firewallu je nemožné. UDP je datagramový protokol, kde každá správa je nezávislá. Naopak filtrovanie TCP spolieha na `ACK` bite na rozlíšenie medzi prichádzajúcou požiadavkou a vracajúcim sa paketom z odchádzajúceho spojenia. UDP nemá podobný indikátor. Možno tak spoliehať na číslo portu zdrojovej stanice, ktorý býva objektom falšovania.

[2]login mechanizmus, pri ktorom jedna strana prezentuje otázku "challenge", napríklad vyžiadanie hesla, a druhá strana musí poskytnúť správnu odpoveď "response", napríklad heslo, k úspešnej autentifikácii.

[3]je technika pre prelomenie šifry alebo autentifikačného mechanizmu, skúšaním určiť jej dekódovací kľúč alebo heslo prehľadávajúc pravdepodobné možnosti.

Čo je horšie, že RPC-based[4] služby používajú dynamické čísla portov. Niekedy aj z vysoko číselného rozsahu, v ktorom nie je port registrovaný. Nepriamo uvedené služby nie sú potom podrobiteľné na ochranu pomocou paketových filtrov.

Dynamické paketové filtre dokážu spárovať odpoveď s požiadavkou. Využívajú timeout na indikáciu, že spojenie je ukončené.

Opatrný postoj naznačuje zakázanie prakticky všetkých odchádzajúcich UDP paketov. Nie že by bola požiadavka nebezpečná, ale nemožno dôverovať odpovediam. Výnimkou sú protokoly poskytujúce peer-to-peer komunikáciu, ktoré jednoducho prijmú odpoveď, pretože majú pevné číslo portu a nie anonymné z vysoko číselného rozsahu.

protocol	out	in	comment
UDP	block	block	*Ťažko rozlíšiť spoofnutú požiadavku od odpovede*

H.323 a SIP

Protokoly H.323 a SIP sú určené pre komunikáciu ľudí po Internete a IP telefóniu. Robustný a komplexný H.323, zastrešujúc radu konkrétnych protokolov, má niekoľko problémov. Vyžaduje zložitý proxy server, ktorý dokáže interpretovať kontrolné správy, a vyžaduje otvorenie ďalších portov, medzi inými aj pre UDP. SIP je oveľa jednoduchší, je iba signalizačným protokolom. Rieši iba nadviazanie a zrušenie spojenia, a má dohľad nad spojením.

protocol	out	in	comment
H.323	block	block	*Používať telefón?*

SMB

Server Message Block je protokol, ktorý naivne predpokladá dôveryhodné prostredie. Poskytuje abstrakciu pre zdieľanie súborov, tlačiarní a iných zariadení. Preto by nemal presahovať bezpečnostný okruh dôveryhodnej siete.

protocol	out	in	comment
SMB	block	block	

3.3 Ďalšie služby [1]

IPsec, GRE, a IP over IP

Všetky z protokolov sú navrhnuté niesť IP v rámci iných protokolov. Inými slovami vytvárajú nový spoj, ktorým možno obísť firewall. Hoci za určitých starostlivo kontrolovaných okolností je to dobrá myšlienka.

[4]remote procedure call predstavuje technológiu, ktorá umožňuje počítačovému programu zavolať podprogram alebo procedúru a spustiť ho v inom adresnom priestore, často na vzdialenom počítači na zdieľanej sieti bez toho, aby programátor explicitne programoval detaily pre túto vzdialenú interakciu

ICMP

Existuje mnoho známych prípadov zneužitia protokolu ICMP hackermi na útoky typu *denial-of-service*[5]. Odfiltrovaním tohto protokolu odopierame užitočné informácie pre riadenie a vykonávanie sieťových diagnostických funkcií. Napríklad `traceroute` závisi na potvrdení `Time Exceed` a `Port Invalid` IMCP paketov.

Niektoré ICMP správy nemôžu byť blokované. Napríklad technika *Path MTU discovery*[6] vyžaduje tieto správy. Ak nie sú povolené, užívatelia siete nebudú schopní komunikovať s určitými sieťami. Falošné `Destination Unreachable` správy môžu viesť k *denial-of-service* útoku, ale ich ponechanie vedie k zlepšeniu výkonu. Cenou získania informácie, že cieľ je nedostupný, je riziko zaplavenia ICMP správami, a tým spadnutie systému a prerušenie spojení.

Povolenie resp. blokovanie protokolu ICMP predstavuje kompromis medzi funkčnosťou a bezpečnosťou. Niektoré *firewalking* techniky používajú Path MTU ICMP správy.

protocol	**out**	**in**	**comment**
ICMP	allow	some	*Path MTU vyžaduje ICMP*

[5]je pokus urobiť zdroj informácii nedostupným pre pôvodne zamýšlaných užívateľov

[6]je technika v počítačových sieťach pre určenie veľkosti maximálnej prenosovej jednotky (Maximal Transmission Unit - MTU) na ceste v sieti medzi IP adresami dvoch staníc, obvykle s cieľom vyhnúť sa IP fragmentácii.

4 Súčasnosť a budúcnosť

Dôležitým faktorom, týkajúcim sa súčasných technológií, je podľa štúdie [17] to, že s rastúcou kapacitou priemerného pripojenia na Internet sa firewally stávajú akýmsi hrdlom (zúženým miestom). Je to zapríčinené vyspelejšími inšpekčnými metódami analyzujúcimi traffic.

Ďalším faktorom, že jednotný firewall s rozličnými funkciami nemá podobu v úspešnom komerčnom i nekomerčnom produkte. Multifunkčné zariadenia sú schopné pracovať priemerne oproti jednoúčelovým, ktoré dokážu spracovávať traffic perfektne.

Firmy, vyvíjajúce firewallové produkty zabezpečenia, namiesto toho, aby zdokonaľovali vlastnú antivírusovú detekciu, postupujú detekciu externému antivírovému programu, bežiaceho ako samostatná aplikácia. Súčasné bezpečnostné systémy sú nejednotné, avšak každý pracuje výborne v danej špecializácii.

4.1 Komerčné firewally

Svetovou firmou, ktorá hrá kľúčovú rolu vo vývoji a poskytuje komplexné riešenia s podporou a vysokou garanciou je spoločnosť CISCO. Pole pôsobnosti zahŕňa sieťové a telekomunikačné technológie a služby.

Ďalšou významnou spoločnosťou pôsobiacou v oblasti sieťového zabezpečenia je KERIO s ponúkanými produktmi MailServer a WinRoute Firewall.

Spoločnosť Symantec má silné meno vo vyvíjaní produktov ako antivírové a antispywarové programy pre koncové stanice - užívateľské počítače.

4.2 Prognóza do budúcnosti

Bude budúcnosť firewallov jednoduchá alebo komplikovaná? Myslím, že záleží, z ktorej strany sa na ňu pozeráme. Pre developerov bude komplikované dosiahnuť integráciu funkcií a technológií do jednej platformy, ktorá je schopná spracovávať traffic s rýchlosťou 10Gbps a väčšou a mať úspešnosť detekcie 100% s výslednou cenou menšou ako €100 pre koncového spotrebiteľa. S prihliadnutím, že hrozba od hackerov sa nedá načasovať, v prípade čo i len náznaku infiltrácie musí výrobca produktu byť pripravený zasiahnuť a vydať update sotfwareu alebo firmwareu.

Zákazníci a používatelia na druhej strane vidia budúcnosť firewallu nasledovne: žiadne červy, vírusy, hackerské exploity, trójske kone, útoky typu denial-of-service ani iné bezpečnostné zlyhania. Personálny firewall vidia v jednoduchosti inštalácie, spravovania, resp. ako súčasť operačného systému, bez potreby akejkoľvek dodatočnej interakcie. Profesionálny užívatelia naopak vyžadujú interakciu zo strany firewallu, chcú mať prehľad o prichádzajúcich a odchádzajúcich spojeniach a možnosť ovplyvniť nastavenia.

Kam sa bude sieťová bezpečnosť uberať v blízkej budúcnosti? Črtajú sa tri možné scenáre: návrat k jednoduchým systémom, čo je však málo pravdepodobné ale technicky uskutočniteľné; vyvinutie nových prostriedkov na spravovanie zložitosti celého problému, čo je ťažko dosiahnuteľné a vyžadovalo by to vynájsť nové techniky; alebo zotrvanie stavu aký je v súčasnosti.[20]

Integrácia

Bude pokračovať oddelený vývoj rôznych bezpečnostných systémov alebo všetko bude integrované? Spoločnosťou, ktorá sa snaží o kompletnú jednoliatu integráciu je Microsoft. Ale táto integrácia skrýva množstvo škaredého ("prasácky" naprogramovaného) za pekný prívetivý interface. Samotný Microsoft sa chváli, že operačný systém Vista obsahuje viac ako 50 miliónov riadkov kódu, čo je o 40% viac ako predchádzajúca verzia, Windows XP. Prečo by sme mali očakávať dokonalú bezpečnosť od jedného z najkomplikovanejších systémov?

Samotný problém integrácie spočíva vo vybudovaní jednoliateho systému a navrhnutí komponentov akými sú firewall, IDS, VPN, host IDS, host integrity checker, antivírusový systém, šifrovací systém, bezpečný Web server od začiatku tak, aby spolupracovali pod spoločným spravovateľným interfaceom.[20]

Zhrnutie

Výsledkom tejto práce a skúmania internetovej a sieťovej bezpečnosti je nasledujúci prehľad princípov zabezpečenia (Z môjho pohľadu uvádzam hodnotenie princípov ako elementárne *, chytré **, geniálne***):

- prístup cez heslá *
- šifrovanie ** (komunikácie, hesiel)
- filtrovanie pomocou smerovača *
- prístup cez aplikačnú bránu **
- prístup cez proxy bránu ** (aplikačná brána so službou proxy)
- zavedenie DMZ *** (v zapojení s jedným, alternatívne dvomi smerovačmi a aplikačnými bránami v nej umiestnených)
- osobný firewall na koncových počítačoch **
- distributed firewall ** (aplikovaný administrátorom pre užívateľov domény, autorizácia prístupu)

Kombinácia predchádzajúcich komponentov sa odzrkadľuje na architektúrach siete, najpoužívanejšími možnosťami sú:

- Screening router * (zapojenie so smerovačom)
- Dual-homed host ** (zapojenie s aplikačnou bránou, monitorujúca komunikáciu)
- Screened host architecture ** (primárne filtrovanie zabezpečuje vonkajší smerovač, služby vo pre vnútornú sieť poskytuje aplikačná brána)
- Screened subnet architecture *** (realizácia myšlienky DMZ, nie však nutne blokovanie priamej komunikácie)

Samozrejme že kto robí, robí aj chyby. A tak každá technológia má aj slabiny, na ktoré sa prišlo až postupným používaním technológie. Identifikovanými problémami, ktoré vyplývajú s používaním vyššie uvedených technologických princípov, ktoré boli spomenuté v tejto práci sú:

- prelomenie hesla (uhádnutie, dictionary attack, brute-force attack)
- prelomenie šifrovania (s využitým súčasnej výpočtovej kapacity a distribuovaného výpočtu na viacerých počítačoch)

- neznalosť prenášanej informácie (napríklad u paketového filtrovania - nespochopnosť porozumieť protokolom vyšších vrstiev neznalosť protokolov vyšších vrstiev)
- zmena hlavičkových informácií paketu (IP spoofing)
- tranzitivita dôvery (problém pri source routingu)
- spomalenie zapríčinené spracovávaním informácií pomocou proxy
- kompromis pri filtrovaní služieb (protokolov a príslušných portov)
- rôznorodosť protokolov a nedostupnosť podpory (pri nastavení akýchkoľvek filtrujúcich pravidiel alebo proxy brány)
- výkon vs. bezpečnosť (všeobecne hĺbková detekcia obsahu paketov niečo stojí)
- zlyhanie ľudského faktora (resp. nezodpovedné správanie sa užívateľov vnútornej siete)
- Denial-of-Service útoky (zahltenie public serverov požiadavkami a zneprístupniť tak služby pre normálne použitie)
- Trójske kone (vytvárajú možnosť neautorizovaného prístupu)

Je úroveň zabezpečenia výsledkom strachu z obídenia bezpečnosti a uskutočnenia možných nelegálnych aktivít, akými sú odcudzenie informácií, modifikácia, alebo zosmiešnenie hackermi? Alebo je úroveň výsledkom bezpečnostných smerníc a noriem? Myslím si, že pokiaľ sa nestane prípad, ktorý by slúžil ako precedens do budúcna, aj pre konkurenčné subjekty, strach nehrá veľkú úlohu.

Skôr si spoločnosť chce chrániť renomé firmy, značku, vyhnúť sa finančnému kolapsu, a nemôže si dovoliť zlyhanie voči svojim klientom. Preto spoločnosti spolupracujú a často vyhľadávajú komplexné riešenia od firiem s dlhodobými skúsenosťami. Preto manažment firmy prihliadne na značku spoločnosti zaberajúcej sa bezpečnosťou.

Je snaha o obídenie bezpečnosti úmerná potencionálnemu zisku? Závisí od toho, či má útočník alebo hacker v úmysle sa obohatiť, alebo mu ide len o poukázanie na slabiny príslušného systému, prípadne o prestíž.

Táto práca mala skúmať internetovú a sieťovú bezpečnosť z hľadiska firewallu, identifikovať slabé a silné miesta. Poukázať na princípy zabezpečenia cez heslá, šifrovanie, filtrovanie trafficu, na využitie aplikačných brán, a uviesť zakomponovanie firewallu do rozdielnych architektúr sietí.

Slovník

CGI skript (Common Gateway Interface) - je štandardný protokol pre prepojenie aplikačného softvéru s informačným serverom (zvyčajne Web serverom)

DMZ zone (delimitarizovaná zóna) - je logická sieť obsahujúca externé služby organizácie a vystavuje ich pre iné nedôveryhodné siete, (napr. Internet), môžu sa v nej napríklad nachádzať Web server, E-mail server a Proxy server

Ethernet - realizuje vrstvu sieťového rozhrania, technológia pre siete LAN

FTP (File Transfer Protocol) - protokol určený na prenos súborov medzi počítačmi cez sieť

GPS (General Positionig System) - navigačný systém zahŕňajúci satelity a počítače, ktoré môžu určiť zemepisnú šírku a dĺžku prijímača na Zemi pomocou výpočtu časového rozdielu od rôznych satelitov dosahujúcich na daný prijímač

GRE (Generic Routing Encapsulation) - tunelovací protokol vyvinutý spoločnosťou CISCO, ktorý môže zapuzdriť celú radu paketov, patriacich protokolom pracujúcim na sieťovej vrstve, do IP tunelov, a vytvoriť tak virtuálne spojenie link-to-link na smerovačoch CISCO na vzdialených miestach pracujúce na IP internetworkingu

HTTP (Hypertext transfer Protocol) - komunikačný protokol na prenos informácii na internete, okrem iného aj publikovanie a získavanie HTML stránok

H.323 - zastrešuje odporúčania od ITU Telecommunication Standardization Sector, ktorý definuje protokoly poskytujúce audiovizuálnu komunikáciu a zabezpečuje reláciu na akekoľvek paketovej sieti

ICMP (Internet Control Message Protocol) - využívaný v sieti pre odosielanie chybových správ, napr. keď požadovaná služba nie je dostupná alebo zariadenie nie je dosažiteľné

IDS (Intrusion Detection System) - softwarový bezpečnostní systém, obecne deteguje nechcené manipulácie počítačových sietí, hlavne cez Internet, nemôže detegovať útoky v zakódovanom spojení

IMAP (Internet Message Access Protocol) - protokol pracujúci na aplikačnej vrstve, obsluhovaný na porte 143, ktorý povoľuje lokálnemu IMAP klientovi pristupovať k e-mailom na vzdialenom servery, aktuálna je verzia IMAP4rev1

IPsec - je protokolová sada pre zabezpečenie IP komunikácie poskytujúc autentifikáciu a šifrovanie pre každý paket dátového streamu

ISP (Internet Service Provider) - poskytovateľ internetového pripojenia, firma alebo organizácia sprostredkujúca prístup do Internetu, poskytujúca telekomunikačné služby

Malware - je všeobecné označenie škodlivého softvéru, patria sem počítačové vírusy, trójske kone, spyware a adware

NTP (Network Time Protocol) - protokol pre synchronizáciu hodín počítačových systémov cez paketovo prepojované siete, s variabilnou latenciou, využíva UDP na porte 123

POP3 (Post Office Protocol) - internetový štandardný protokol pracujúci na aplikačnej vrstve, používa lokálnych e-mailových klientov na vyzdvihnutie e-mailov zo vzdialeného servera cez TCP/IP spojenie

Router - je sieťové zariadenie (smerovač), sprostredkováva prenos dát medzi dvomi alebo viacerými sieťami, smeruje a preposiela informácie

SIP (Session Initiation Protocol) - signalizačný protokol, používaný na zostavenie a zrušenie multimediálnej komunikačnej relácie využívanej na Voice a Video hovory cez Internet (VoIP).

Source Routing - povoľuje odosielateľovi paketu špecifikovať cestu, ktorou má byť smerovaný, celá cesta k cieľu je známa, od ostatných smerovaní sa odlišuje tak, že zdroj rozhoduje o smerovaní pre každý router pozdĺž cesty, technika je používaná na úrovni linkovej vrstvy (aj napriek tomu, že smerovanie naznačuje sieťovú vrstvu)

Subnet - je rozsah logických adries v rámci adresného priestoru priradeného organizácii, adresa uzlov v subnete začína binárnou sekvenciou ID siete a ID subnetu, identifikuje ho adresa a maska subnetu, používa sa na rozdelenie siete do menších viac efektívnejších subnetov

Spyware - špehovací program, ktorý sa bez vedomia užívateľa pokúša získať citlivé dáta a odoslať prostredníctvom internetu tretej strane

VPN (virtual private network) - privátnosť je vytvorená určitou metódou virtualizácie, prepojenie počítačov na rôznych miestach Internetu do jednej počítačovej siete, počítače sa môžu nachádzať vo fyzicky nezávislých sieťach

Literatúra

[1] William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin : *Firewalls and Internet Security: Repelling the Wily Hacker*, Second Edition, Addison-Wesley, 2003, ISBN 020163466X.

[2] *Evolution of the Firewall Industry*, Cisco, 2002.
`http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm`

[3] Angus Wong, Alan Yeung: *Network Infrastructure Security*, Springer, 2009, ISBN: 978-1-4419-0165-1.

[4] Jiří Peterka: *Počítačové síte*, Prednášky na MFF UK v Praze, 2008.

[5] Jiří Peterka: *Gateway* `e-archiv.cz`

[6] Jiří Peterka: *Bezpečnost na Internetu*, `e-archiv.cz`.

[7] Kenneth Ingham, Stephanie Forrest: *A History and Survey of Network Firewalls*, Univeristy of New Mexico, 2002.

[8] Talal Alkharobi, *Firewalls*, slides, 2007.
`http://ocw.kfupm.edu.sa/user062/CSE55101/firewall.pdf`

[9] *Firewall Toolkit*, FWTK documentation.
`http://www.fwtk.org/fwtk/docs/documentation.html#1.1`

[10] D. Brent Chapman: *Network (in)security through IP packet filtering*, Proceedings of the Third USENIX UNIX Security Symposium, 1992.

[11] David W. Chapman Jr., Andy Fox: *Zabezpečení sítí pomocí Cisco PIX Firewall*, Computer Press, 2004, ISBN: 80-722-6963-1.

[12] Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman: *Building Internet Firewalls*, Second Edition, O'Reilly, 2002, ISBN: 1-56592-871-7.

[13] `http://en.wikipedia.org/wiki/Firewall_(networking)`

[14] `http://en.wikipedia.org/wiki/Application_layer_firewall`

[15] `http://en.wikipedia.org/wiki/Protocol_stack`

[16] `http://en.wikipedia.org/wiki/Personal_firewall`

[17] David Cartwright: *The Future of Firewalls: Where is firewall technology going?*, Techworld, 2003.
`http://www.techworld.com/security/features/index.cfm?featureid=196`

[18] Cisco. http://www.cisco.com/.

[19] Kerio. http://www.kerio.cz/.

[20] Interview with Marcus J. Ranum: *Firewall pioneer: Security needs integration*. INDUSTRY WATCH TOOLKIT on ZDNet UK. 2003.
http://news.zdnet.co.uk/itmanagement/0,1000000308,2129769,00.htm

Zoznam obrázkov