SHKOLLA E MESME “SEZAI SURROI” BUJANOC
PROFILI ARSIMOR: ELEKTROTEKNIK I KOMPJUTERËVE

PUNIM MATURE

Tema: MURET MBROJTËSE (FIREWALL-ËT)

Lënda: RRJETAT KOMPJUTERIKE DHE KOMUNIKIMI

Profesori i lëndës
ABAZ MEMETI, inxh. dip.

Nxënësi
SEJAD DEMIRI, IV$_7$

Qershor, 2012

Përmbajtja

1.HYRJE

Në fillim të këtij punimi duhet të theksohet se muret e zjarrta dhe muret mbrojtëse janë plotësisht terme identike. Shfaqja e qasjes brezgjerë në Internet ka krijuar përvojë të jashtëzakonshme për administratorët e rrjetave kompjuterike. Qasja e shpejtë ka hap rrugë për inova-cione të shumta në fushën e këmbimit të të dhënave, qasjes së pajisjeve dhe teknologjive tjera më të avancuara kompjuterike. Fatkeqësisht, kjo teknologji gjithashtu ka krijuar edhe mundësi të lehtë të qasjes nga brendësia e çdo rrjete, e me këtë edhe të çdo kompjuteri në rrjetë.

Ashtu si rrjetat bëhen më komplekse, gjithashtu edhe sulmuesit tentojnë të infiltrohen në ato. Siguria e rrjetit tani nuk është vetëm mbrojtje e serverit dhe stacioneve punuese. Sot, ajo kërkon kuptimin e detajuar të rrjetit dhe njohjen me cenueshmërinë e rrjetit, si në bërthamën e saj ashtu edhe në pjesët e skajshme.

Ashtu si sulmuesit janë bërë më të sofistikuar, gjithashtu janë avancuar edhe veglat që i përdorin sulmuesit për tu infiltruar në rrjeta. Këto vegla, në shumicën e rasteve janë falas, ofrohen në Web faqe të ndryshme, ku i mundësojnë edhe shfrytëzuesve me arsimim më të ultë të sulmojnë rrjeta. Sot sulmet në rrjeta i bëjnë fillestarët informatik, konsumatorët e zemëruar, ish të punësuarit ose ata që donë të shohin se çka mund bëjnë.

Të gjitha këto ndryshime kanë shkaktuar përkeqësimin e punës për ti siguruar rrjetat nga sulmet. Gjithashtu është rritur edhe numri i pajisjeve që duhet mbrojtur. Administratorët e sigurisë sot duhet të vlerësojnë se a bëhet fjalë për një sulm të vërtet të dikujt, i cili din se çka po vepron, apo ndonjë shkollar provon ndonjë përkrahje të re programore për DoS (angl. *denial of service*) sulme.

Muri mbrojtës (angl. *firewall*) bëhet pikë ngulfateshe në rrjetë, ai definon se kujt ti besohet, e kujt jo. Pjesët e dyshimta të rrjetit janë të gjitha, nga rrjeta e jashtme (Interneti), e deri tek disa departamente në organizata, varësisht nga arkitektura e tërësishme e rrjetit. Muret mbrojtëse të sotshme kanë evoluar më shumë se në vet pikën ngulfateshe. Përmbajnë zgjidhje të llojllojshme: fizike-harduerike, programore-softuerike, personale-humane, detektim të ndërhyrjes, etj. Me zhvillimin e teknologjisë, rritet edhe numri i mundësive që i ofron shfrytëzuesve muri mbrojtës.

2. Muri mbrojtës (Firewall)

Muri mbrojtës e zgjidh problemin e sigurisë në këtë mënyrë: parandalon çdo komunikacion të tillë me rrjetën lokale për të cilën konsiderohet se mund të jetë e dëmshme, apo thjeshtë – e panevojshme. Muri mbrojtës kryesisht vendoset në atë vend ku pjesa e sigurt e rrjetit lidhet në Internet, siç është treguar në **figurën 1**.

I gjithë trafiku që vije dhe shkon nga ajo zonë e mbrojtur kalon përmes murit mbrojtës i cili vendos se a është trafiku i pranueshëm apo jo. Për pranueshmërinë e ndonjë lloji të trafikut (porosi e-mail-i, transferim të të dhënave, operim të kompjuterit nga largësia, etj.) vendoset në bazë të politikës së sigurisë të vet rrjetit. Politika e sigurisë të çdo kompjuteri apo rrjeti të mbrojtur dallohet varësisht prej interesave dhe qëllimeve të vet organizatës apo individit.

Mund të themi se muri mbrojtës ka rolin e filtrit. Për shembull, muri mbrojtës mund ti refuzoj (ti hedh poshtë) të gjithë ato pakete/porosi (në vend që ti përcjell) që vinë nga rrjeta e jashtme dhe të cilët i përkasin ndonjë IP adresës së rrjetit lokal[1], dhe/ose ndonjë porti TCP[2]. Muri mbrojtës mund t'i refuzoj paketat/porositë në bazë të IP adresës së dërguesit dhe me këtë ti pamundësoj ndonjë entiteti (nyejve, proceseve, komunikatorëve) të vendosin komunikim me nikoqirët nga rrjeta lokale që e mbron/ndanë ai mur mbrojtës nga pjesa tjetër e rrjetës.

Implementimi fizik i murit mbrojtës shpesh varion dhe varet kryesisht nga kërkesat e shkallës së sigurisë të buxhetit që është në dispozicion. Më së shpeshti ai është grup i komponentëve fizike – ruterëve (angl. router), kompjuter të lidhur në rrjetë publike dhe pajime të përshtatshme programore. Për të arritur shfrytëzuesi deri te pjesa e mbrojtur e rrjetit nevojitet që së pari ta kaloj murin mbrojtës dhe përmes tij të qaset në rrjetin publik.

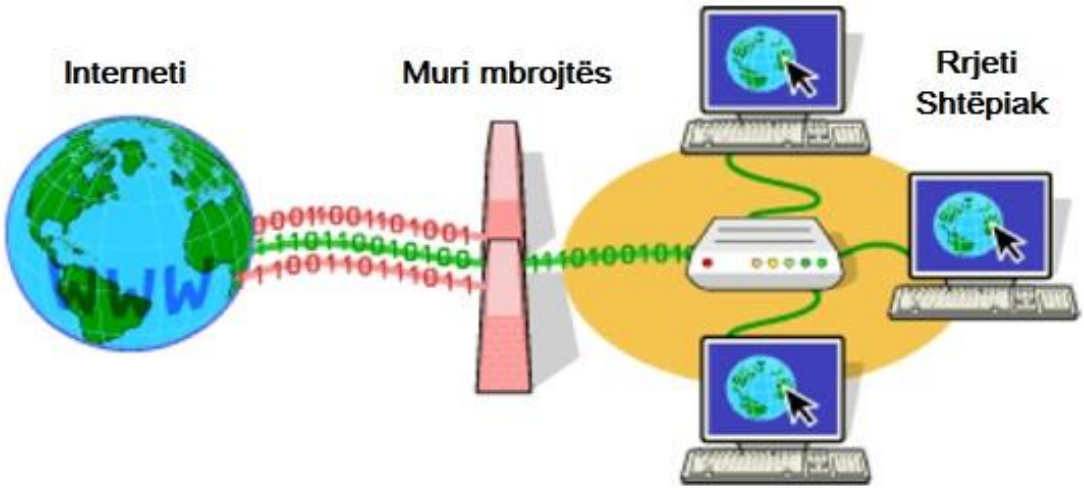

Figura 1. *Muri mbrojtës i bazuar në aplikimin e filtrit*

[1] Numri IP apo IP adresa është numër-simbol unik i kompjuterit në Internet
[2] Porti TCP – protokollët që sigurojnë këmbim të të dhënave ndërmjet kompjuterëve, ku përmes numrit të portit identifikohet se cilit aplikacion programor të kompjuterit i përcillen të dhënat

2.1. Llojet e mureve mbrojtëse

Muret mbrojtëse zakonisht ndahen në dy klasë themelore edhe atë: muret mbrojtëse të bazuar në aplikim të filtrit (*filter-based*) dhe muret mbrojtëse të bazuar në aplikim të proxy-t.

2.1.1. Muri mbrojtës i bazuar në aplikim të filtrit

Muret mbrojtëse të bazuar në aplikim të filtrit përmbajnë tabela të adresave dhe porteve, në bazë të të cilave vendos se cilët pakete/porosi do ti përcjell e cilat do ti hedh poshtë. Figura 1 tregon murin mbrojtës të bazuar në aplikim të filtrit.

Në përgjithësi, çdo rresht i kësaj tabele përmban katër parametra themelor, edhe atë: IP adresën dhe portin TCP portin e burimit dhe IP adresën dhe portin TCP të destinimit, ndërkohë këto parametra mund të jenë të shënuar në mënyrë që të simbolizojnë tërë klasat e adresave apo porteve. Këto të dhëna në tabela mund të përdoren për atë që të pengoj komunikimin ndërmjet adresave/nyejve dhe porteve, ose të lejohet komunikimi (vetëm) ndërmjet adresave/nyejve dhe porteve të cekura, ndërsa të parandalohen të gjitha komunikimet tjera.

2.1.2. Muri mbrojtës i bazuar në aplikim të proxy-t

Serveri proxy – në përgjithësi është kompjuter i cili qëndron si ndërmjetës në mes klientit dhe serverit kryesor.

Në mënyrë specifike, serverët proxy më së shpeshti përdoren për shërbime të web faqeve, përkatësisht përdorim të Internetit. Ekziston Proxy-server i thjesht dhe reverzibil.

Skema klasike është organizatë e madhe në të cilën ekziston numër i madh i kompjuterëve, e punonjësit zakonisht në mëngjes përveç leximit të postës elektronike shfletojnë edhe horoskopin ditor. Zakonisht në mëngjes faqet e Internetit të gazetave ditore janë të mbingarkuara.

Nëse në kompjuter (gateway, router) përmes të cilit të gjithë qasen në Internet vendoset programin që horoskopin vetëm një herë do ta kërkoj nga serveri fundor, e gjithë të tjerët do ti shërbej nga memoria e saj, të gjithëve do ti shpejtohet *surfimi*. **Figura 2** në mënyrë të përkryer sqaron murin mbrojtës të bazuar në aplikim të proxy-t.

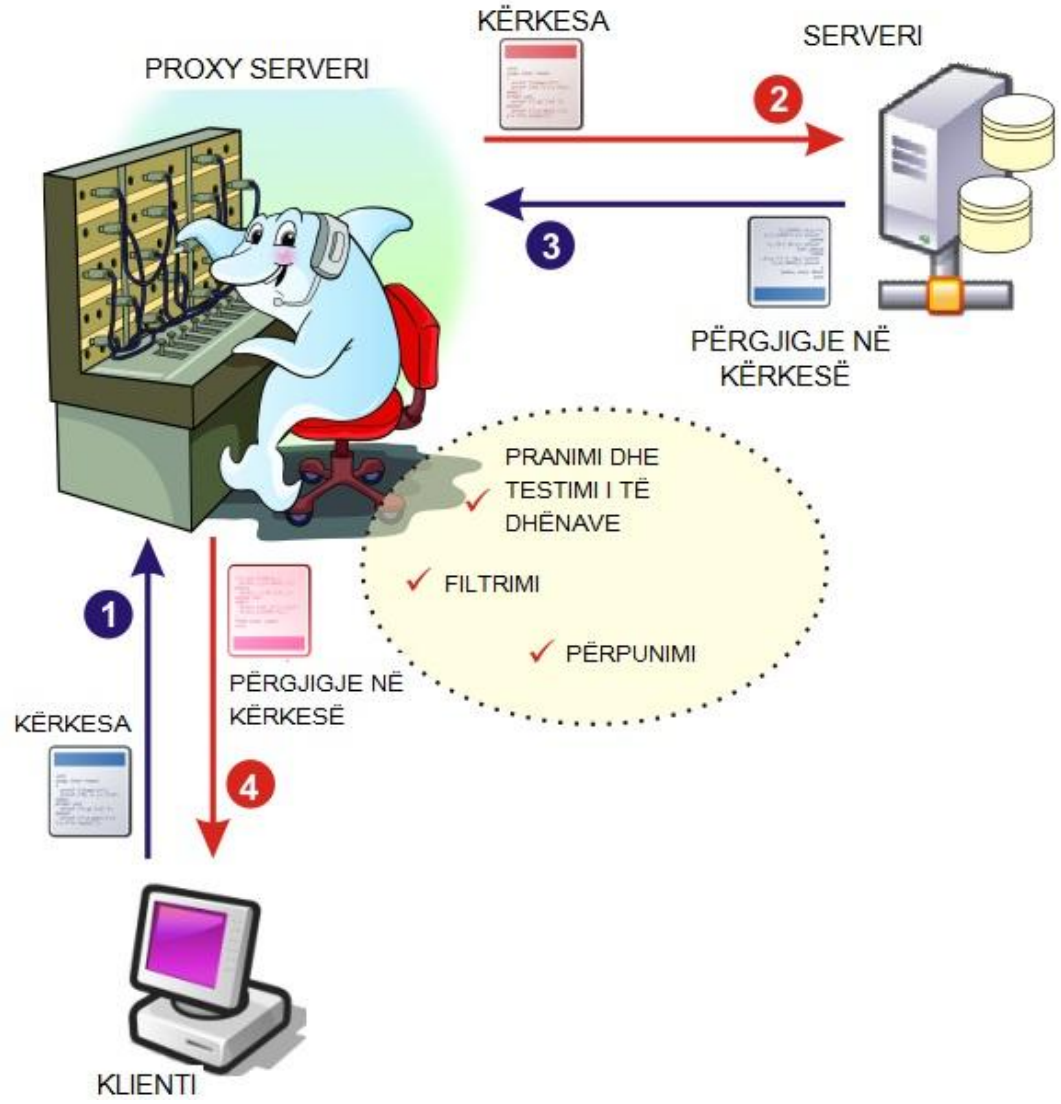

Figura 2. *Muri mbrojtës i bazuar në aplikim të proxy-t*

3. Ndërtimi i mureve mbrojtëse

Në ndërtimin e mureve mbrojtëse nuk mund të angazhohet çdokush. Zakonisht, në këto projekte kyçen administratorët e sistemeve ose individë tjerë që i njohin rrjetat kompjuterike dhe në përgjithësi që e njohin strukturën e rrjetave, e gjithashtu e njohin edhe rrjetin që synojnë ta sigurojnë me mur mbrojtës. Ky proces nuk është i thjeshtë, ndërsa disa hapa kryesor që duhet respektuar janë:

- Njohja e rrjetit dhe protokolleve të nevojshëm
- Zhvillimin e rregullave të caktuara
- Posedimin e materialit adekuat

- Shfrytëzimin e veglave në mënyrë efikase
- Testimin e konfigurimit
- Njohjen e rrjetit dhe rregullave tjera

4. Muret mbrojtëse komerciale

Në këtë pjesë do ti përmendim dy mure mbrojtëse të cilat janë shumë të përshtatshme, andaj edhe çdo shfrytëzues duhet ti posedoj.

Zone Alarm / Zone alarm PRO

Zone Alarm / Zone alarm PRO është jashtëzakonisht "miqësisht" i inkurajuar ndaj shfrytëzuesve. Paralajmërimet janë përshkruese. Ndoshta edhe nuk është më i miri për profesionistët, sepse duket shumë i thjeshtë. Për amatorët nuk ka program më të mirë. ZoneAlarm është mur mbrojtës i vetëm i cili përveç tendencës për të hyrë në kompjuterin e shfrytëzuesit, shqyrton edhe programet që dërgojnë informacione nga kompjuteri i shfrytëzuesit. Kjo është shumë e rëndësishme nëse rastësisht keni kali të trojës[3].

BlackICE defender

Nëse jeni gjahtar të kokave, ky është mur mbrojtës të cilin duhet ta posedoni. Nuk ju lodh me pyetje se çka të veproni, por vetvetiu tenton ti zbuloj kërcënimet në kompjuterin tuaj. Arsyeja më e madhe e lavdisë së këtij programi është se jo vetëm që i bllokon sulmet, por i ruan dhe i zbulon informacionet për sulmuesit.

[3] Sikur miti i kalit të trojës që dukej si dhuratë, e në fakt barte në vete ushtar grek të cilët e pushtuan Trojën, kuajt e sotshëm të trojës janë programe që duken si vegla të dobishme, po në të vërtet kërcnojnë sigurinë dhe shkaktojnë dëme shumë të mëdha. Së fundmi kali i trojës vije në formë të porosisë së postës elektroike me skeda të bashkangjitur të cilat pretendohen të jenë azhurime të sigurisë për Microsoft, e në të vërtet janë virus të cilët pamundësojnë programet antivirus dhe softuerët e murit mbrojtës.

5. Përfundim

Zona e studimit që përfshin muri mbrojtës, përkatësisht muri i zjarrtë, si pjesë e sigurisë së kompjuterëve, është shumë e gjerë dhe shpesh e thurur me teknologji tjera që ofrojnë siguri të kompjuterëve dhe rrjetave kompjuterike.

Prandaj ky punim mature është vetëm një njoftim me disa nga mundësitë e sigurisë. Duhet theksuar se muret mbrojtëse nuk ofrojnë siguri të plotë nga virusët dhe nga të dhënat e dëmshme, çka paraqet mangësinë më të madhe të tyre.

Fatkeqësisht, na ndjek fakti se shumë organizata dhe njerëz të paditur nuk dëshirojnë shtojnë të reja në punën e tyre, dhe në punën e tyre i përcjell thinja: “Kam punuar kësisoj dhjet vite, pse mos të vazhdoj edhe më tutje”. Për shkak të mendimit të këtillë ekziston mundësi më e madhe e infektimit të të gjithë shfrytëzuesve tjerë të Internetit, e të gjithë e dimë se si ndikojnë virusët në kompjuterët tanë.

6. LITERATURA:

http://spvp.zesoi.fer.hr/seminari/2004/firewall-ssutic.pdf

http://www.microsoft.com/croatia/security/virus.mspx

http://osnove.tel.fer.hr/nastavnici/randic/oum/Seminar0405/Security.pdf

http://dev.mysql.com/tech-resources/articles/proxy-overview.png

Zoran Urošević: Računarske Mreže i Komunikacije, ZAVOD, Beograd 2008.

Shënime nga lënda: RRJETAT KOMPJUTERIKE DHE KOMUNIKIMI, Bujanoc 2011/2012.