

# Eldveggir

Sjálfstætt verkefni í Tölvuöryggi

Háskólinn í Reykjavík, Tölvunarfræðideild, Haustönn 2004.

Leiðbeinendur: Dr. Gísli Hjálmtýsson og Björn Brynjúlfsson.

Nemandi: Sigurjón Sveinsson.

## 1 Inngangur

Internetið er opið allri netumferð og litlar hömlur eru á henni aðrar en tæknilegir örðugleikar á borð við bandvídd og tafir í nethnútum. Mikið frelsi fylgir þessu og hver sem er getur svo gott sem gert hvað sem er á Internetinu.

En frelsinu fylgja þeir gallar að það er margt á internetinu sem ógnar öryggi tölvunotenda og tölvukerfa. Hakkarar brjótast inn í tölvukerfi og gera árásir á þau, vírusar dreifa sér milli tölva og óumbeðinn tölvupóstur (spam) flæðir um allt. Til þess að sporna við þessu eru m.a. notaðir eldveggir.

Í þessari greinargerð verður fjallað um eldveggi, hvaða hlutverki þeir gegna, hvernig þeir virka og gegn hverju þeir vernda okkur.

xxx

## 2 Hlutverk eldveggja

Eldveggur er hugbúnaður eða vélbúnaður sem skoðar netumferð sem flæðir milli internetsins og staðarnets og beitir aðgerðum á þá umferð samkvæmt fyrirfram ákveðnum öryggisskilgreiningum. Eldveggur getur einnig verið hugbúnaður sem fylgist með netumferð á einmenningstölvum til að hefta útbreiðslu orma og vírusa og verja tölvuna sjálfa gegn slíkum netárásam. Með því að setja eldveggi milli internetsins og staðarneta geta kerfisstjórar staðarnetanna stjórnað því hvernig netumferð flæðir milli þessara neta. Hægt er að loka á netumferð eftir því hvaða tölvur, eða mengi tölva, eiga í hlut, eftir því hvers konar samskiptastaðall er notaður við samskiptin og einnig eftir því á hvaða þjónustu umferðin beinist. Einnig getur eldveggur beint ákveðinni netumferð frá internetinu á ákveðna tölvu eða tölvur á staðarneti.

Eldveggir geta verið hluti af stýrikerfi og þar með innbyggðir. Sem dæmi má nefna iptables og ipchains í Linux og Internet Connection Firewall í Windows XP. En það eru mörg fyrirtæki sem framleiða sérstaklega eldveggi, hvort sem það er hugbúnaður (t.d. Symantec, Zone Labs og Kerio Technologies) eða vélbúnaður (t.d. Cisco, WatchGuard, DSL beinar).

## 3 Virkni eldveggja

Með því að skoða hvern einasta pakka af gögnum sem er að flæða til og frá staðarneti og bera þá saman við skilgreiningar eldveggjarins, sem geymdar eru í skrá eða gagnagrunni, getur eldveggurinn tekið á þeim samkvæmt þeim skilgreiningum. Eldveggurinn getur hent pökkunum, hleypt þeim í gegn og beint þeim inn á ákveðna vél á staðarnetinu [1,2].

### 3.1 Aðferðir við að sía pakka

Eldveggir nota eftirfarandi aðferðir við að skoða pakka og stjórna flæði á netumferð inn og út úr staðarneti.

#### 3.1.1. Pakkasíun (e. Packet Filtering)

Hver pakki, einn og sér, er skoðaður og borinn saman við færslur í töflu. Þeim pökkum sem komast í gegnum færslurnar er hleypt í gegn en öðrum er hent.

Kostir pakkasíunnar eru að það er frekar einfalt að útfæra hana sem þýðir að það er ólíklegra að hægt sé að nota öryggisgalla í útfærslu eldveggjarins. Vegna þessa einfaldleika verða allar reglur um meðhöndlun á pökkum mun einfaldari og því minni líkur að þær séu rangar og innihaldi galla.

Helstu gallar við pakkasíun er að TCP pakkar eru einungis síaðir eftir því hvaða port þeir eru að fara á. Einnig er ekki hægt að ábyrgjast það að pakkar komist ekki í gegn sem ekki eru gildir pakkar eða ekki hluti af gildri TCP tengingu. Á sama hátt er ekki heldur hægt, með fullnægjandi hætti, hægt að sía UDP pakka til að tryggja það að þeir séu hluti af gildri tengingu [1].

#### 3.1.2. Stöðubundin skoðun (e. Stateful Inspection)

Stöðubundin skoðun tekur grundvallaratriði í pakkasíun og bætir við það sögu gagna. Þetta þýðir að eldveggurinn skoðar pakkann með hliðsjón af sögu fyrri pakka. Með þessari aðferð er hægt að stjórna netumferð betur fyrir samskiptastaðla sem pakkasíun tekur ekki nógu vel á eins og t.d. UDP. Einnig er hægt að stjórna betur flæði netpakka.

Það er flóknara að útfæra stöðubundna skoðun og þar af leiðandi eykst hættan á því að útfærslur séu gallaðar. Einnig krefst stöðubundin skoðun meira minnis og kröftugri örgjörva í þeim vélbúnaði sem eldveggurinn er á vegna þess að eldveggurinn þarf að geyma gögn um hverja tengingu í ákveðinn tíma [3].

#### 3.1.3. Application-level síun

Eldveggir geta tekið á fleiri vegu en einungis eftir IP tölum og portum sendanda og móttakanda. Þeir geta tekið á pökkum eftir því fyrir hvaða forrit þessir pakka eru. T.d. er hægt að sjá hvort TCP pakki innihaldi tölvupóst og geti þá tekið á honum á vissan hátt. Nefna að application-level eldveggur getur skilið RFC 822 hausa, MIME formuð viðhengi og gæti líka borið kennsl á vírusa í tölvupósti [1].

Einn stærsti kostur þess að nota application-level síun er að það er hægt að skrá og stjórna allri netumferð. Tölvupóstur getur t.d. verið skoðaður og athugað með stikkorðaleit hvort að verið sé að senda trúnaðarupplýsingar og hægt er að taka í burtu hættuleg viðhengi á borð við keyrsluskrár (.exe) [1].

Helsti gallinn við application-síun er að hún þarf að nota sérhannaðan hugbúnað fyrir mismunandi gerðir netumferðar. Tölvupóstur krefst t.d. annars hugbúnaðar en ftp forrit. Einnig getur verið erfitt að skoða umferð fyrir mjög sérhæfð forrit.

## 3.2 Þættir sem ákvarða meðhöndlun á pökkum

Þegar pakki kemur að eldvegg, hvort sem hann kemur frá staðarnetinu eða internetinu, er skilgreint hvað á að gera við hann. Þessar skilgreiningar segja til um hvort það eigi að eyða honum, svara honum eða senda áfram inn á innranetið og þá hvert.

Ef eldveggurinn er á vefþjóni og það kemur UDP pakki á porti 53 (DNS) sem vefþjónninn bað ekki um þá er sennilega skilgreint í eldveggnum að þessi pakki sé ekki viðeigandi og honum er hent.

Ef eldveggurinn er á beini fyrir staðarnet (Default Gateway), pósthjónninn er fyrir innan eldvegg og það kemur tölvupóstur á porti 25 þá geta þeir pakkar verið sendir áfram á pósthjónninn og einungis hann.

Ef pakkinn er fyrir vefsíðu sem vél fyrir innan eldvegginn bað um, og eldveggurinn hefur notað NAT (sjá umfjöllun síðar) til að áframsenda fyrir vélina, þá getur eldveggurinn séð að þessi pakki er í raun fyrir vél fyrir innan eldvegg og sendir pakkann til hennar.

### 3.2.1. Hvaðan pakkinn kemur

Hver einasti hnútur sem tengdur er internetinu er með einkvæma IP tölu. Að sama skapi er hver einasti hnútur á staðarneti með einkvæma IP tölu. Eldveggur getur skoðað hver sendandi hvers pakka er og skilgreint hvort hleypa eigi pakkanum inn/út eftir því. Að sama skapi er hægt að skilgreina lén sem sendanda, því lén er í rauninni bara nafn sem á bak við er IP tala.

### 3.2.2. Hvaða samskiptastaðlar pakkinn er á

Það eru til margir samskiptastaðlar á internetinu og hver hefur sín eigindi og hlutverk. Hægt er að taka á pökkum og sía þá eftir því hvaða samskiptastöðlum þeir eru á. Þessir staðlar geta verið [2]:

- **IP** (Internet Protocol): Aðalburðarlagið.
- **TCP** (Transport Control Protocol): Brýtur niður og setur saman gögn sem send eru á internetinu.
- **HTTP** (Hyper Text Transfer Protocol): Samskiptastaðall fyrir vefþjóna.
- **UDP** (User Datagram Protocol): Notað til að flytja gögn sem krefjast ekki svars eins og að streyma tónlist og kvikmyndir.
- **ICMP** (Internet Control Message Protocol): Stjórnar tengingum milli hnúta ásamt fleiru.
- **SMTP** (Simple Mail Transport Protocol): Samskiptamáti tölvupósts.

### 3.2.3. Hvaða þjónustu pakkinn er fyrir

Allar þjónustur og forrit sem nethnútar nota, hvort sem það eru þjónar, einkavélar eða beinar, nota svokölluð port til að tilgreina sig. Þessi port eru skilgreind sem númer og getur hvert port aðeins verið notað fyrir eina þjónustu í einu á hverjum hnút. Þannig geta ekki tveir vefþjónar (t.d. Tomcat og Apache) verið í gangi í einu á sömu vél og verið að nota sama portið (80). Fyrstu 1024 portin eru frátekin fyrir algengar og vel þekktar þjónustur og er hægt að sjá hverjar þær eru á vefsíðunni [http://en.wikipedia.org/wiki/List\\_of\\_well-known\\_ports\\_\(computing\)](http://en.wikipedia.org/wiki/List_of_well-known_ports_(computing)).

### 3.2.4. QoS

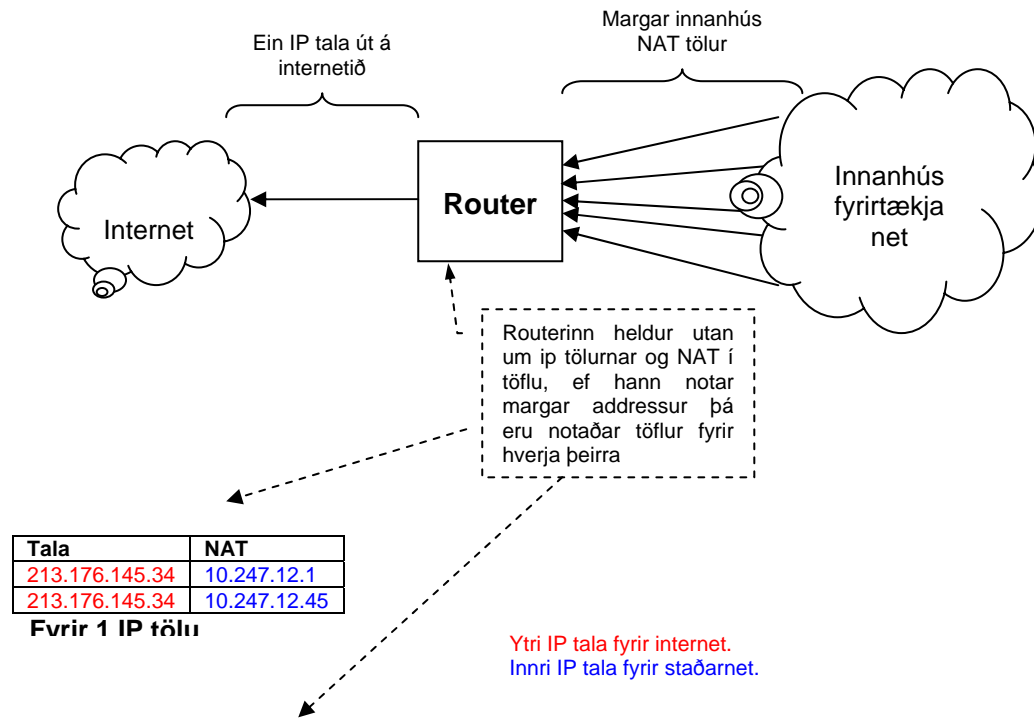
Sumir eldveggir bjóða uppá þjónustutryggingu (e. Quality of Service) sem tryggir að ákveðnir hnútar eða samskiptastaðlar fái alltaf ákveðna þjónustu sem lofuð er. Þessi þjónusta getur verið hraði, bandvídd, gagnamagn, aðgengi og fleira. Með þessari þjónustu er hægt að veita ákveðnum pökkum forgang í hnútum svo ekki komi tafir á mikilvægar gagnasendingar.

## 4 NAT

NAT (e. Network Address Translation) er ekki tækni hönnuð fyrir eldveggi heldur í raun hentug lausn á takmörkuðum fjölda af IP tölum á internetinu [3].

NAT var gert til að maska eða hjúpa net á bak við eina IP tölu á Internetinu. Þetta er gert til að spara úthlutunir IP talna hjá internetþjónustuaðilum. Þegar IP pakkar fara í gegnum nethnútt sem notar NAT út á internetið skiptir nethnúturinn um uppruna IP tölu og uppruna port á pakkanum og sendir áfram á IP tölu viðtakanda, t.d. vefþjón. Nethnúturinn skráir þessar breytingar í NAT töflu hjá sér. Vefþjónninn svarar beiðninni og sendir svarið á IP tölu nethnútsins sem snýr að internetinu. Þegar pakkinn kemur að nethnútinum flettir hann upp í NAT töflunni og skoðar hver upphaflegur eigandi að sendingunni er á innra netinu. Nethnúturinn skiptir um IP tölur aftur, s.s. endastöðvar IP og port og sendir áfram.

Það eru mjög skiptar skoðanir á NAT í netheimum, sumir eru þeirrar skoðunnar að NAT brjóti lagskiptingu nethögunnar. Port séu stíluð á ferli á application laginu og að breyta þeim á network laginu brjóti högunina. Nethnútar eigi ekki að fara upp fyrir network lagið. Einnig að NAT brjóti transparency högun því að að nethnútar séu að breyta IP pökkum sem endastöðvar eru að senda sín á milli.



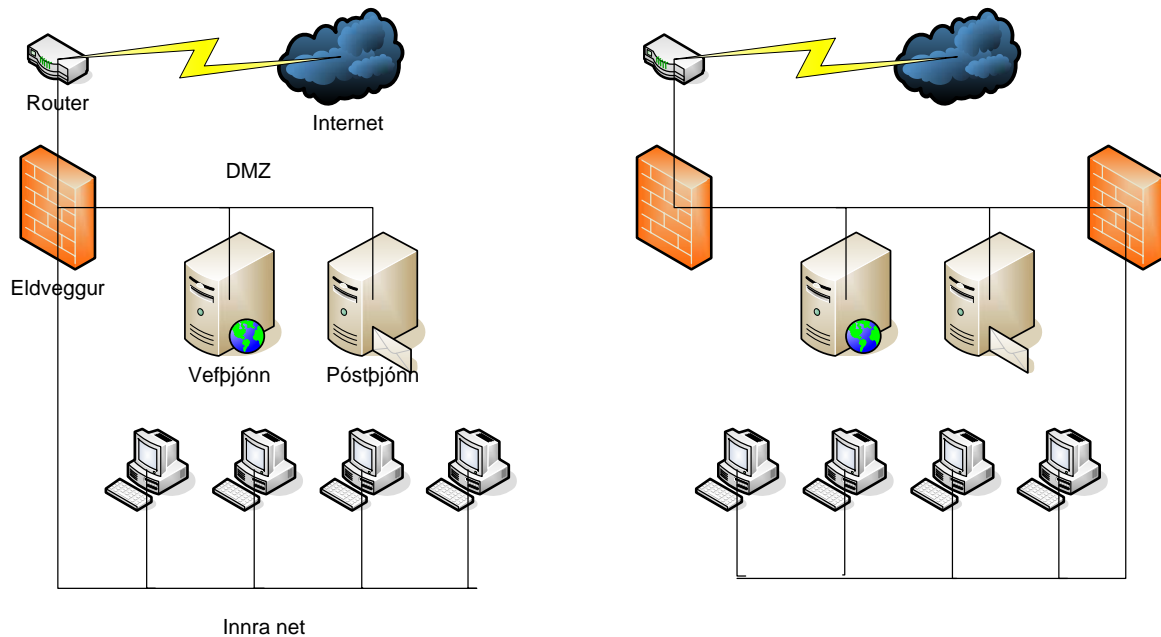
Tala	NAT	Tala	NAT	Tala	NAT
213.176.145.34	10.247.12.1	213.176.145.35	10.247.11.2	213.176.145.36	10.247.10.3
213.176.145.34	10.247.12.45	213.176.145.35	10.247.11.3	213.176.145.36	10.247.10.5

Dæmi: Fyrir margar IP tölur. Aðskildar IP tölur fyrir aðskilin innri net.

## 5 DMZ

Sumar uppsetningar á staðarnetum eru þannig að þjónustur sem þurfa að vera aðgengilegar frá internetinu, eins og vefþjónustur og tölvupóstur, eru settar á vélar sem eru fyrir innan eldvegginn, þ.e. eru í raun á innranetinu. Eldveggur netsins er síðan stilltur þannig að þegar beiðni kemur á eldvegginn um að komast í þessa þjónustu er þeirri umferð hleypt í gegnum eldvegginn. Við það að stilla eldvegginn þannig að hann hleypi beiðnum frá internetinu inn á innranetið skapast öryggisáhættur.

Til að stemma stigu við þessari áhættu er sett upp svokallað DMZ (e. Demilitarised Zone) sem hefur reyndar ekkert með hernað að gera. DMZ er svæði þar sem netþjónar eru geymdir og tengdir, sem keyra þjónustur sem þurfa að vera aðgengilegar frá internetinu og eru hluti af netrekstri þess innranets sem IP tala eldveggjarins er fyrir. En aðgangur frá þessum þjónum inn á innranetið er lítill sem enginn.



DMZ með einum eldvegg.

DMZ með tveim eldveggjum.

DMZ er hægt að framkvæma með einum eldvegg eða tveimur. Ef einn eldveggur er notaður þá er eldveggurinn stilltur þannig að hann sýar út alla netumferð milli staðarnetsins og DMZ nema þá allra nauðsynlegustu [2,3].

Ef tveir eldveggir eru notaðir er ráðlagt að nota ekki sama hugbúnað né vélbúnað á þessa eldveggi. Það er ekki algengt að tölvuprjotar brjótist inn á eldveggi en það gerist. Sé brotist inn á ytri eldvegginn þá eru minni líkur að innri eldveggurinn sé í hættu ef hann er öðruvísi.

Það eru kostir og gallar að nota einn eldvegg í DMZ. Það er einfaldara og þar af leiðandi er allt utanumhald minna. Allar öryggisskilgreiningar verða þar með einfaldari. Einnig er ódýrara að nota einn eldvegg en tvo. En gallinn snýst um svokallaðan "single point of failure". Ef brotist er inn á eldvegginn er allt staðarnetið opið fyrir prjótinn.

## 6 Heimildaskrá

- [1] William R. Cheswick, Steven M. Bellovin og Aviel D. Rubin, 2003. *Firewalls and Internet Security, Second Edition*.
- [2] Jeff Tyson, *Howstuffworks: How Firewalls Work*. <http://www.howstuffworks.com/firewall.htm>
- [3] Rob Pickering, *Internet Firewall Tutorial*. <http://www.rpanetwork.co.uk/wp/fw.rhtm>