ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՆՎՏԱՆԳ ԱՊԱՀՈՎՈՒՄԸ FIREWALL-Ի ՕԳՆՈՒԹՅԱՄԲ

ՄԻՐԻԲՅԱՆ ԱՐԹՈՒՐ
ԳՊՀ տեղեկատվական տեխնոլոգիաների բաժնի մասնագետ,
Ինֆորմատիկայի և ֆիզիկամաթեմատիկական
գիտությունների ամբիոնի դասախոս
e-mail: a.miribyan@gsu.am
ԱՊԿԱՐՅԱՆ ԼՈՒԻԶԱ
ԳՊՀ բնագիտական ֆակուլտետի համակարգչային
ճարտարագիտություն բաժնի
3-րդ կուրսի ուսանողուհի
e-mail: luizaapkaryan@gmail.com

Ժամանակակից աշխարհում անձնական տվյալների անվրանգ ապահովումը առաջնային տեղ է գրավում:

Հոդվածում լուսաբանվում է, թե ինչպես Firewall-ի /հրդեհային պատի/ միջոցով ապահովել անհատական համակարգչի անվտանգությունը: Ներկայացվում է նաև, թե ինչպես Firewall ծրագրային կամ ապարատային բլոկի միջոցով իրականացնել վերահսկում և ցանցային փաթեթների զտում՝ խուսափելու համար վիրուսներից և արտաքին ցանցային հարձակումներից:

Բանալի բառեր՝ *Firewall, ինֆորմացիա, անձնական տվյալներ, ծրագրային ապահովում, տվյալների շտեմարան:*

Երբ խոսվում է համակարգչային անվտանգության մասին, օգտագործողների մեծամասնությունը դա կապում է համակարգչային վնասակար վիրուսների հետ: Բայց վիրուսները միակ խնդիրը չեն. հաճախ օգտագործողները ուշադրություն չեն դարձնում այն փաստի վրա, որ նույնիսկ հակավիրուսային ծրագրակազմի առկայության դեպքում կորցնում են անհրաժեշտ տվյալներ՝ չնայած այն բանին, որ հակավիրուսային ծրագիրը անընդհատ համակարգչում կատարում է զննում: Կամ մեկ այլ դեպք՝ ինտերնետի ծավալը /лимит Интернета/, որը նախատեսված է մեկ ամիս օգտագործելու համար և մի քանի օրվա ընթացքում սպառվում է:

Ո՞րն է այս տարօրինակությունների պատճառը: Բացատրությունը պարզ է: Ինչպես գիտեք, ինտերնետ հասանելիությամբ յուրաքանչյուր անհատական համակարգիչ (ԱՀ) ունի յուրահատուկ IP հասցե: Այն 4 մասից բաղկացած մի թվաշարք է, որոնցից յուրաքանչյուրը կարող է լինել 0-ից մինչև 255: Համակարգչին անհրաժեշտ է IP հասցե՝ ցանկացած այլ համակարգչի հետ համացանցում «շփվելու» համար: Ամեն օր համակարգիչը կապի է դուրս գալիս բազմաթիվ համակարգիչների հետ և դրանց

միանում է համապատասխան կցիչների /պորտերի/ հասցեների միջոցով: Այս պարագայում համակարգիչը դառնում է բավականին խոցելի: Վտանգավոր իրավիճակներից խուսափելու համար անհրաժեշտ է արգելափակել համակարգչի հաղորդակցումը կասկածելի բոլոր կցիչների հետ՝ օգտագործելով համապատասխան ծրագրակազմը (firewall):

Առաջին firewall-ները ի հայտ են եկել դեռ 1980-ականներին: Դրանք սովորական երթուղիչներ էին, որոնք ներառում էին փաթեթների զտիչներ /filtr/: Ըստ տրված կարգավորումների՝ ստուգվում էին փոխանցվող տվյալները, և անհամապատասխանության դեպքում ինֆորմացիոն հոսքն արգելափակվում էր: 1990-ականներին հայտնվեցին այսպես կոչված՝ շղթայական մակարդակի firewall-ները: Բարդությամբ և նորույթով հաջորդում են ծրագրային մակարդակի «պաշտպանները» /"защитники" программного уровня/: Հետագայում փաթեթների դինամիկ զտումը դարձավ firewall-ների հիմքը: Մերօրյա firewall-ների հիմքը նորագույն ճարտարապետության kernel proxy-ի ծրագիրն է (այս ճարտարապետությունն ունի ինչպես ծրագրային, այնպես էլ ապարատային ներդրումներ):

Firewall (անգլերենից թարգմանաբար նշանակում է հրդեհային պատ, կրակե հատված), հաճախ նաև հանդիպում է բրենդմաուեր /brandmauer/ անունով, որը գերմաներենից նույնպես թարգմանաբար նշանակում է հրդեհային պատ: Սա հատուկ ծրագիր է, որը ակտիվացվում կամ ապաակտիվացվում է տվյալ համակարգչի օգտագործողի կողմից՝ պաշտպանելով համակարգիչը արտաքին միջամտությունից:

Այլ կերպ ասած՝ Firewall-ը պատնեշ է համացանցի և համակարգչի միջև: Այս ծրագիրը վերահսկում է համակարգիչների միջև եղած կապը, վերլուծում դրանք և որոշում կայացնում՝ թույլ տա՞լ տվյալ կապակցումը, թե՞ ոչ: Այսինքն՝ ծրագիրը թույլատրում է օգտագործողի կողմից հաստատված կապերը: Firewall-ը վերահսկում է ոչ միայն մուտքային, այլ նաև ելքային կապերը, այսինքն՝ նույնիսկ եթե վիրուսը ինչ-որ կերպ ներթափանցել է համակարգիչ և փորձում է համացանցի միջոցով անձնական տվյալների արտահոսք կատարել, firewall-ը կկանխի այդ փոխանցումը և օգտատիրոջը կզգուշացնի այդ մասին, ինչպես նաև ոչ ոք չի կարող մուտք գործել համակարգիչ և որևէ տեղեկատվություն փոխանցել 3-րդ անձի:

Firewall-ը կարող է համացանց «բաց թողնել» կամ համացանցից ներբեռնել միայն այն ծրագրերը, որոնք թույլատրված են օգտագործողի կողմից: Բոլոր մյուս չհաստատված ծրագրերը երկկողմանի կապերի ժամանակ արգելափակվում են:

Համակարգչային առավելագույն պաշտպանության համար անհրաժեշտ է ընտրել համապատասխան կարգավորումներ: Առաջարկվում է թույլատրել կապը միայն այն ծրագրերի հետ, որոնք անհրաժեշտ են: Առաջին հայացքից սա բարդ է թվում, բայց firewall-ներում կան կարգաբերման օգնականներ, որոնք հուշումների միջոցով պար-

զեցնում են կարգաբերման գործընթացը: Կարևոր է ուշադիր հետևել ընթացքում ծրագրի կողմից տրվող հրահանգներին:

Firewall-ը ունի երկու՝ անձնական և կորպորատիվ պատեր: Անհատական պատը ծրագիր է, որը տեղադրված է անհատական համակարգչում, իսկ կորպորատիվ պատը տեղադրվում է համացանցի և տեղային ցանցի միջև ընկած դարպասի /шлюз/ վրա: Անհատական firewall-ն ունի ներկառուցված օգնական-հրահանգիչ, որի օգնությամբ հեշտությամբ կարելի է հասկանալ ծրագրի աշխատանքը և կարգաբերել ըստ համապատասխանության: Եթե համակարգչում որևէ ծրագիր կասկածելի է, firewall-ն ուղարկում է համակարգային հաղորդագրություն, և օգտագործողն ինքն է որոշում կայացնում՝ թույլատրե՞լ, թե՞ արգելափակել տվյալ ծրագիրը: Կան տարատեսակ անձնական firewall-ներ, որոնցում ընտրության հնարավորությունը մեծ է: Նրանք տարբերվում են տեսակներով, միջավայրերով /интерфейс/, լինում են վճարովի և անվճար: Բայց, ըստ էության, բոլորն էլ կատարում են միևնույն գործառույթը: Կորպորատիվ firewall-երը կարգաբերվում են համակարգի ադմինիստրատորի կողմից, որն ամբողջ ցանցը պաշտպանում է հարձակումներից:

Firewall-ը սերվերի վրա կամ գլոբալ ցանցում տեղադրվում է որպես առանձին սարք, միևնույն ժամանակ հնարավոր է տեղադրել նաև որպես համալիր ծրագրակազմ:

Firewall ծրագրի գործառույթը կարելի է ստուգել՝ օգտագործելով Leak Test ծառայությունը:

Firewall-ի շահագործման ռեժիմները

Proxy firewall

Proxy firewall-ը միջնորդ է օգտվողի ԱՀ և իրական սերվերի միջև: Բոլոր կապերը տեղի են ունենում Proxy firewall-ի անունից: Կապ հաստատելու համար ներքին ցանցի սերվերները հարցում են ուղարկում firewall-ին, որն այնուհետև ստացված հարցման հիման վրա նախաձեռնում է նոր կապ: Հարցումները համեմատվում են կանոնների բազայի հետ. եթե հարցումը չի պարունակում արգելված պարամետրեր, ապա firewall-ը կազմում է փաթեթ, որում ներկայացված է լինում հարցումը: Արտաքին սերվերից պատասխան ստանալուց հետո firewall-ը ստուգում է այն, և եթե պատասխանը համապատասխանում է պահանջներին, այն փոխանցում է հաճախորդի հասցեին, որն էլ ի սկզբանե կատարել էր հարցումը: Հարցումը իրականացվում է բազմաթիվ պարամետրերի հիման վրա. ուղարկողի և ստացողի IP հասցեները, միջանկյալ սարքերի առկայությունը, հարցումների ժամանակը և այլն:

Proxy firewall-ը ամենահուսալի տեսակներից մեկն է: Proxy firewall-ը իրականացնում է զտում, գրանցում և վերահսկում, հարցումներ՝ անվտանգության բարձր մակարդակ ապահովելու համար: Հանգույցների միջև ինֆորմացիոն փաթեթների ուղիղ փոխանցման բացակայության դեպքում պաշտպանում է IP հասցեները և էապես նվազեցնում է վտանգի հավանականությունը հարձակվողներից, որոնք կա-

րող են որոշել ներքին ցանցի տոպոլոգիան՝ ելնելով փոխանցվող փաթեթներում պարունակվող տեղեկատվությունից: Proxy firewall-ը կատարում է տեղեկատվության պահպանում, ինչը թույլ է տալիս նվազեցնել երթևեկի ծավալը և կրճատել հաճախորդի տեղեկատվություն ստանալու ժամանակը: Ի տարբերություն փաթեթային զտիչների Proxy firewall-ների ֆիլտրման կանոնները պարզ են:

Reverse Proxy Firewall

Reverse Proxy Firewall-ը գործարկվում է այնպես, ինչպես Proxy firewall-ը մեկ սկզբունքային տարբերությամբ՝ այն օգտագործվում է բացառապես սերվերները պաշտպանելու համար:

Reverse Proxy Firewall սերվերը հաճախորդի հարցումը ստանում է ամբողջովին, իսկ մշակման համար մասամբ կամ ամբողջությամբ փոխանցում է այլ սերվերների: Արդյունավետությունը բարելավելու համար հարցումները կարող են փոխանցվել բազմաթիվ սերվերների՝ այդպիսով նվազեցնելով ընդհանուր բեռը:

Reverse Proxy Firewall գործում է վեբ սերվերի անունից և հաճախորդների համար տեսանելի չէ: Երբ անցանկալի հարցում է ստացվում, սերվերը խնդիրը չլուծելու դեպքում այն չի ուղարկում հաճախորդին, այլ անցանկալի հարցումը ինքնուրույն վերահղում է այլ սերվերի և ստացված պատասխանը վերադարձնում հաճախորդին: Այսպիսով՝ Reverse Proxy Firewall-ը սովորական վեբ սերվեր է՝ մի քանի լրացուցիչ հատկություններով, ներառյալ URL-ի վերահղումը:

Trasparent Firewall

Trasparent Firewallը հայտնի է նաև որպես Bump in the Wire: Այն նաև քեշ սերվեր է, սակայն բացառում է հաճախորդի կողմից կարգաբերումները: Trasparent Firewall-ը տեղակայված է ենթացանցի ներսում՝ ցանցի անցուղու վրա: Դրա շնորհիվ այն հնարավորություն ունի զտելու ենթացանցը: Այս դեպքում հաճախորդը նույնպես տեղյակ չէ Trasparent Firewall-ի գոյության մասին, հետևաբար, հաճախորդի ԱՀ-ը կարիք չունի հիշելու կամ գրանցելու սերվերում Firewall-ի պարամետրերի կարգաբերումը:

Next Generation Firewall

Firewall-ների շուկան շարունակ զարգանում է, արտադրողները գործառույթներ են ավելացնում՝ անվտանգության բարձրացման և սպառնալիքներին առավել համապարփակ դիմակայելու համար: Next Generation Firewall-ները (NGFW) ցանցային անվտանգության հարթակներ են, որոնք իրենցից ներկայացնում են ավանդական firewall-ներ՝ ներխուժման կանխարգելման համակարգերով (IPS) համալրված, մուտքի վերահսկման մշակման քաղաքականությամբ, զտելու, ինֆորմացիոն հոսքի խորը վերլուծություն անելու (DPI) և կիրառման նույնականացման հնարավորություններով: Նման ծրագրային համակարգերը թույլ են տալիս հայտնաբերել և արգելափակել ամենաբարդ գրոհները:

Այսպիսով՝ հաջորդ սերնդի firewall-ները պետք է ապահովեն.

• ծրագրերի շարունակական վերահսկում, պաշտպանություն հարձակումներից և ներխուժումներից,

• երկու տարբեր օգտագործողների համակարգերի ինտեգրվելու հնարավորություն,

• ծրագրերի նկարագրության և հնարավոր սպառնալիքների պարբերաբար թարմացվող համակարգ:

Ամպային տեխնոլոգիաների զարգացմանը զուգընթաց աճում է նաև հաջորդ սերնդի firewall-ների պահանջարկը:

Firewall-ի առկայությունը համակարգում, ճիշտ կարգավորման դեպքում, թույլ է տալիս պաշտպանել անձնական տվյալների փոխանցումը երրորդ անձի, ինչպես նաև պաշտպանել սերվերները հարձակումներից: Իհարկե, մեր օրերում ոչ ոք չի կարող բացարձակ երաշխիք տալ, բայց եթե ինչ-որ մեկը փորձի ներխուժել ձեր համակարգիչ, firewall-ը նրա համար կլինի շոշափելի խոչընդոտ:

Օգտագործված գրականություն

1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. — ИНФРА-М, 2011. — 416 с. — ISBN 978-5-16-003132-3.

2. Фаронов А. Е. Основы информационной безопасности при работе на компьютере. — ИНТУИТ, 2016. — 155 с.

3. Лапонина О. Р. Межсетевое экранирование. — Бином, 2014. — 343 с. — ISBN 5-94774-603-4.

Կայքերի հղումներ

1. http://freeprotection.ru/kak-rabotaet-fajrvol/,
2. https://www.dataarmor.ru/firewall-types/,
3. https://en.wikipedia.org/wiki/Firewall_(computing),
4. https://www.forcepoint.com/cyber-edu/firewall,

SAFE INFORMATION SECURITY WITH FIREWALL

MIRIBYAN ARTUR
IT specialist,
Lecturer at the Chair of Informatics and Physical-Mathematical Sciences,
GSU
APKARYAN LUIZA
3rd year student,
Faculty of Natural Sciences
Department of Computer Engineering, GSU

In the modern world, protection of personal data is on the first place. This article explains how to ensure the safety of your PC through a firewall. It also shows how to control and filter packets through the Firewall programs and hardware block, avoiding viruses and unwanted network attacks.

Keywords: *Firewall, information, personal data, software, database.*

БЕЗОПАСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИИ С ПОМОЩЬЮ FIREWALL

МИРИБЯН АРТУР
Специалист отдела Информационных технологий ГГУ,
Преподаватель кафедры информатики и физико-математических наук
АПКАРЯН ЛУИЗА
Студентка 3-его курса отделения «Компьютерная инженерия» ГГУ

В современном мире безопасное обеспечение персональных данных занимает первостепенное место, и в статье освещается, как с помощью FIREWALL (пожарной стены) обеспечить безопасность персонального компьютера. Представляется как с помощью программного обеспечения, так и с помощью аппаратного блока Firewall осуществлять контроль и фильтрацию сетевых пакетов, чтобы избежать вирусов и внешних сетевых атак.

Ключевые слова: *Firewall, информация, личные данные, программное обеспечение, база данных.*

Հոդվածը ներկայացվել է խմբագրական խորհուրդ 04.09.2020թ.:
Հոդվածը գրախոսվել է 14.10.2020թ.: