6-шы дәріс Ресурстарды сүзгілеумен жұмыс істеу әдістері.

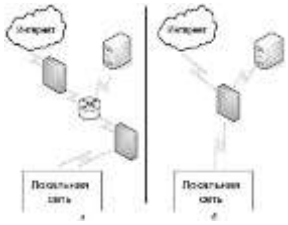
Қазіргі заманғы ақпараттық жүйеде әр түрлі міндеттер әр түрлі санаттағы ақпаратпен үйлеседі, ал қауіп көбінесе ұйымның периметрі бойынша емес, оған қол жеткізе алатын қолданушылар тарапынан туындайды. Сондықтан әрбір автоматтандырылған жүйе жалпы ақпараттық жүйенің бөлігі ретінде желіаралық экранмен қорғалуы керек.

Демилитаризацияланған аймақ

Әдетте демилитаризацияланған аймақ (Demilitarizedzone, DMZ) ұғымы - бұл ресурстары Интернетте жариялануы керек компьютерлерді білдірді.

DMZ - бұл интернеттен де, жергілікті желідегі компьютерлерден де желіаралық экранмен бөлінген жергілікті желінің арнайы ұйымдастырылған ішкі желісі (сурет 5.2). Желінің осы конфигурациясымен жарияланған қызметі бар компьютерді бұзған шабуылдаушыға басқа жергілікті ресурстарға қол жеткізу өте қиын, тіпті мүмкін емес.

DMZ аймағын екі желіаралық экранның көмегімен жасауға болады (сурет 5.2,а) немесе үш желілік адаптері бар бір желіаралық экранның көмегімен (сурет 5.2,б). Екінші нұсқа арзандау болғанымен, оны орнатуға көп уақыт кетеді және үнемі әкімшінің назарын аударуды қажет етеді.



Сурет 5.2.
Демилитаризацияланған аймақты құру нұсқалары: а –екі желіаралық экранды қолдану арқылы; б –бір желіаралық экранды қолдану арқылы

Демилитаризацияланған аймақ ұғымы бүгінде академиялық мәнге ие. Желіаралық экрандармен тек сыртқы желіден кіруге болатын жүйелерді ғана емес, барлық серверлер мен жұмыс станцияларын қорғау қажет.

Желіаралық экран (брандмауэр)

Желіаралық экран (ЖАЭ) немесе брандмауэр (firewall) - бұл бір желіні екінші желіге қауіпсіз қосу үшін техникалық, программалық және ұйымдастырушылық шаралардың жиынтығы. Шешілетін міндеттерге және қорғалған ақпараттың құпиялылығына байланысты, бұл компьютерде орнатылған шағын программа немесе белгілі бір ұйымның талаптарын орындайтын мамандандырылған арнайы жабдық болуы мүмкін.

Брандмауэр не істей алады және одан не күтуге болмайды?

Брандмауэр жіберілген деректерді де, алынған ақпаратты да сүзеді. Бұл сізге берілген желі үшін қажет емес пакеттерді кесіп тастауға және сыртқы трафикті тек белгіленген компьютерлерге бағыттауға мүмкіндік береді. Брандмауэрлер жергілікті желінің ішкі құрылымын жасырады.

Сонымен қатар, желіаралық экран рұқсат етілген қызметтерде болуы мүмкін және шабуылдаушының жергілікті желіге енуі үшін қолданатын «осал тұстастардан» еш қорғамайды. Мысалы, трояндық вирус танымал тегін FTP серверінің нұсқаларының біріне еніп, оған серверді басқаруды тоқтатуға мүмкіндік бергені белгілі мысал болды. Желіаралық экран арқылы жергілікті желі ресурстарына қосылуға мысал «Желіаралық экран арқылы қосылу» тарауында келтірілген.

Ескерілетін сүзгілеу параметрлері

желіаралық экранның белгілі бір жүйесіне байланысты жіберілетін деректерді сүзудің түрлі нұсқаларын жүзегеасыруға болады, атап айтқанда:
- тәулік уақыты мен апта күндеріне байланысты деректердің өтуіне тыйым салу немесе ашу;
- нақты көрсетілген хаттамалардың өтуіне рұқсат беру;
-жіберушінің немесе алушының адресіне байланысты ақпаратты сүзгілеу;
-жіберушінің аутентификациясының нәтижелеріне байланысты деректерді жіберуге рұқсат беру;
- ақпараттың мазмұнына байланысты деректерді сүзгіден өткізіп барып алу

Бұл параметрлердің әр түрлі комбинациясы болуы мүмкін: сіз қызметкерлердің белгілі бір шеңберіне Интернет-хосттардың белгілі бір тізімімен жұмыс істеуге тыйым сала аласыз немесе баннерлік жүйелер жасаған жарнаманы парақтардағы «бос» орындарға ауыстыра аласыз. (сурет 5.3) KerioWinRouteFirewall желіаралық экран параметрлерін конфигурациялауға арналған терезе мысал ретінде ұсынылған, ол Интернет-парақтарға сұраныстарды бұғаттайтын кілт сөздерді анықтайды.

Сурет 5.3.
Желіаралық экран арқылы контентті сүзгілеу

Сонымен қатар, әдетте желіаралық экрандардың бірқатар қосымша қызмет көрсету мүмкіндігі бар: олар сізге жұмысты хаттамалауды ұйымдастыруға (пайдаланушылардың интернет-трафигін, адрестерін, көлемін және басқаларын есепке алу), сыртқы желіден келетін шабуылдарды анықтап, бұл туралы тиісті

шаралар қабылдау үшін әкімшіге хабарламалар жіберуге, Интернетке кіруді басқаруға және т.б.

Желіаралық экрандарды ұйымдастырудың нұсқалары

Дәстүрлі брандмауэрлерде қолданылатын барлық сүзгілеу әдістерін шартты түрде пакеттік сүзгілеуге және сессия немесе программа деңгейіндегі шлюздерді пайдалануға бөлуге болады. Көп жағдайда нақты жүйелер осы опцияларды біріктіреді.

Пакеттерді сүзгілеу

Пакеттерді сүзгілеу кезінде деректерді қабылдауға / жіберуге рұқсаттар тек IP-адресті және пакет көзінің порт нөмірін және оның тағайындалуын талдау негізінде беріледі. Бұл опция – желіаралық экранды іске асырудың ең қарапайым және жылдам тәсілі.

Ескерту: Негізінде мұндай желіаралық экранды «алдаудың» мүмкіндіктері бар, мысалы, пакеттердегі адрестерді бұрмалау арқылы.

Шлюздер

Сессия деңгейіндегі шлюздер белгілі бір ережелер негізінде клиент пен интернет хост арасындағы уақытша байланыстарды ұйымдастырады. Мұндай арнаны құрғаннан кейін, ол арқылы берілетін барлық ақпарат еркін өтеді. Сессия аяқталғаннан кейін арна жойылады

Шлюздерді ұйымдастырудың тағы бір тәсілі – қолданбалы деңгейдегі шлюздер (көбінесе прокси-серверлер деп аталады), олар жетілдірілген болып саналады. Прокси-серверлер әдетте сұраныстарды қабылдайды (желіден тыс және желі ішінен), пайдаланушының аутентификациясын жасайды, сұраныстарды талдайды және оларды мазмұнға қарай бағыттайды (мысалы, белгілі бір сұранысты ішкі веб-серверге бұғаттайды, ал басқасын тиісті құрылғыға жібереді). Шын мәнінде, клиент пен интернет-хост арасында екі байланыс тізбегі пайда болады: клиенттен прокси-серверге және прокси-серверден интернет-хостқа дейін. Осылайша, ұйымның ішкі ресурстарына тікелей қол жеткізуге тыйым салынады және барлық трафик прокси-сервер атынан шығыс (кіріс) болып саналады.

Прокси-серверлер пайдаланушыларды аутентификациялаудың дамыған мүмкіндіктеріне ие, олардың жұмысын тіркеудің жақсы механизмдері бар және жергілікті желіні қорғаудың ең жоғары деңгейін қамтамасыз етеді.

IntrusionPreventionSystems

Жоғарыда сипатталған трафикті сүзгілеу әдістері, белгілі бір ережелерге сәйкес "жақсы" пайдаланушыларға (немесе қызметтерге) кіруге және "жаман" пайдаланушылар мен қызметтерге тыйым салуға мүмкіндік береді. Бұл тәжірибе біртіндеп тиімділігін жоғалта бастады, себебі зиян келтіруші кодтар

қолданыстағы қорғаныс әдістеріне қарай "бейімделе" бастады. Мысалы, кез-келген программаға ғаламдық желінің кез-келген серверіне компьютерде "қаралған" деректерді беру үшін Интернетке кіру рұқсатын пайдалануға не кедергі келтіреді?
Егер компанияның қызметі жаһандық желімен тығыз байланысты болса, онда клиенттерге қызмет көрсетуден бас тартуды көздейтін оның серверлеріне желілік шабуылдар миллиондаған шығындарға әкелуі мүмкін.

Кәсіпорынның инфрақұрылымына осындай басып кіруді болдырмау үшін күдікті белсенділікті анықтау үшін желі арқылы берілетін пакеттердің мазмұнын бақылайтын аппараттық және программалық шешімдерді қолдана бастады. Бастапқыда мұндай жүйелер желіні негізгі құрылғыларға параллель басқарды және күдікті деректер анықталған кезде қауіп сигналдарын берді. Олар IntrusionDetectionSystems (IDS) деп аталды.

Шабуылдарды болдырмаудың заманауи жүйелері — IntrusionPreventionSystems (IPS) – белсенді функцияны орындайды. Олар шабуылды анықтап қана қоймай, күдікті трафикті бірден бұғаттайды. Мұндай жүйелер dos шабуылының дайындығын анықтай алады, пайдаланушылар арасында деректерді беру үшін қолданылатын программалардың трафигін бұғаттай алады (мысалы, Kazaa, Gnutella, ICQ және т.б.), желілік зиянкестерді (червь), эксплуатациялық белсенділікті және т.б. анықтай алады (сурет. 5.4).

Сурет 5.4.
Nortoninternetsecurity пайдаланушының компьютеріне енуді бұғаттады

IPS жұмысының принципі, ең алдымен, желі арқылы берілетін ақпаратты зиянкестер (червьтер) таратқан пакеттерде, программалық жасақтаманың белгілі бір осалдығын пайдаланатын программалық жасақтама пакеттерінде және т.б. болатын алдын-ала белгілі сигнатуралармен салыстыруға негізделген. Сигнатуралардың құрамы үнемі IPS әзірлеушілерінің веб-сайттарынан жаңартылып тұрады. Сонымен қатар, IPS трафиктің ауытқуын анықтай алады (мысалы, пакеттің бір түрінің күрт көбеюі) және "пайдалы" деректер үшін арнаның өткізу қабілеттілігін сақтай алады.

Деректер пакетінің мазмұнын талдау кезінде ескерілетін сигнатуралар санының артуына байланысты құрылғыға жүктеме артып, нәтижесінде оның өткізу қабілеті төмендейді, сондықтан ұйымның барлық желілік трафигін сенімді қорғау мүмкін емес. Мысалы, CiscoIntrusionDetectionSystems функциясы iOS SoftwareRelease 12.0-ден бастап Cisco коммутаторларының vpo-мен қосылған

(сурет 5), бірақ өндіруші шабуылдардың алдын-алу саясатындағы сигнатуралар саны көбейген кезінде құрылғының жұмысының төмендейтіні туралы ескертеді. IPS шекаралық нүктелерде қолданылады: интернет пен ұйымның жергілікті желісінің қиылысында, сервер сегменті мен пайдаланушы бөлігі арасында.
IPS шекаралық нүктелерде қолданылады: Интернет пен ұйымның жергілікті желісінің түйіскен жерінде, сервер сегменті мен қолданушы бөлігі арасында.

Жоғарыда айтылғандай, шабуылдардың алдын алу технологиялары программалық немесе аппараттық-программа болуы мүмкін. Мысалы, жаңа буындағы CheckPoint – бұл әлемдегі ең ірі компаниялардың көпшілігі өз ресурстарын қорғау үшін пайдаланатын желіаралық экран, оған трафикті талдауға арналған SmartDefense технологиясы кіреді. Сонлай-ақ, Tipping Point (www.tippingpoint.com), Internet Security Systems (www.iss.net), Radware (www.radware.com), TopLayer (www.toplayer.com) және т.б ұсынған арнаулы шешімдер бар.

Осы кластағы шешімдерді қолдану бір жағынан кәсіпорын шығындарын едәуір арттырады және екінші жағынан әкімшілердің дайындығы жоғары болуы керек. Шағын кәсіпорындар үшін мұндай қосымша шығындар әдетте ақталмайтындықтан, олар дәстүрлі брандмауэр программаларын пайдаланады. Сонымен бірге, бұл функционалдылық қауіпсіздік мәселелерімен айналысушы вендорлардың антивирус программаларына енгізіле бастады.

Желіаралық экрандардың нұсқалары

Әкімшілердің иелігінде аппараттық желіаралық экрандармен қатар программалық шешімдер де бар. Осы екі нұсқаның арасындағы айырмашылық өте шартты. Аппараттық модуль – бұл белгілі бір тапсырмаға мамандандырылған бір немесе басқа есептеу жүйесі. Ол үшін әдетте Операциялық жүйе жасалады (мысалы, Cisco-дағы IOS) немесе Linux-тың тегін нұсқасы қолданылады.
Программалық жасақтама нұсқалары типтік операциялық жүйелерге орнатуды көздейді, мысалы: Linux-те, Microsoft операциялық жүйелерінде және т.б

Аппараттық шешімдер

Бүгінгі күні шағын бизнес үшін ең арзан шешім - ол аппараттық желіаралық экрандар. (олардың құны 200 доллардан аз). Мұндай модельдерді коммутациялық жабдық өндірушілердің бәрі шығарады. Сондай-ақ, бір корпуста ADSL модемі мен желіаралық экран сияқты күрделі шешімдер де бар. Құрылғының күрделілігіне байланысты олардың желіні қорғау деңгейлері де әртүрлі. Тіпті ең арзан модельдердің өзіне пакеттерді статикалық сүзгілеу, DMZ порттар, VPN қосылымдарын құру мүмкіндігі, DHCP серверімен NAT тарату, әкімшінің ескерту құралдары (e-mail жіберу және т.б.) секілді қызметтер кіреді.

Windows XP/7/Server 2003/2008 кірістірілген желіаралық экраны

Windows операциялық жүйелерінде кірістірілген желіаралық экран бар. Windows XP-мен салыстырғанда, Windows 7-де трафикті кіріктірілген құралдармен сүзгілеу мүмкіндігі кеңейтілген. Енді пайдаланушылар кіріс үшін ғана емес, шығыс трафик үшін де ережелер жасай алады. Сонымен қатар, жүйеде желіаралық экранның үш профилі бар. Біреуі жеке желіге, екіншісі қоғамдық желіге қосылған кезде, үшіншісі Windows доменінде жұмыс істеген кезде қолданылады. Профильдер – бұл тиісті желі жағдайында жұмыс істеу үшін оңтайландырылған ережелер жиынтығы (профиль қазіргі уақытта компьютер жұмыс істейтін желінің сипаттамаларына байланысты таңдалады). Профильдердің санын өзгерту мүмкін емес, бірақ пайдаланушы белгілі бір Профильдегі құрамы мен конфигурация ережелерін өзгерте алады.

Әр профильде кіріс және шығыс трафиктер үшін әдепкі ережелер бар. Олар деректер пакеті үшін нақты ереже болмағанда қолданылады. Шығыс трафик үшін барлық профильдер үшін әдепкі ереже бәріне мүмкіндік береді, кіріс трафик үшін бәрін бұғаттайды. Сіз бұл параметрлерді өзгерте аласыз, мысалы компьютерден желіге деректердің берілуіне жол бермеу үшін. Бұл жағдайда қажетті деректерді сыртқа тасымалдауға мүмкіндік беретін ереже құру керек.

Әдепкі бойынша, профильде Microsoft желісіндегі компьютердің жұмысын қамтамасыз ететін рұқсат етілген ережелер жиынтығы бар. Ережелер жиынтығы өте көлемді, бірақ Windows-ті орнатудың бастапқы кезеңдерінде өндіруші ұсынған параметрлерді сақтауға болады.
Операциялар шебердің басшылығымен орындалады (сурет. 5.5); оларды орындау аса қиын емес.

WindowsVista-да шығыс трафигі үшін ережелер жасау мастері

Келесі сәттерге ерекше назар аударғым келеді.

Программа, қызмет немесе порт үшін ереже жасауға болады. Мүмкін болса, сізге программаны немесе қызметті таңдау керек. Себебі, порт желіаралық экран жұмыс істеп тұрған кезде жасалған Ережемен ашылады, ал егер ереже программа үшін жасалса, онда порт сол программа жұмыс істеп тұған кезде ғана ашылады. Әрине, бұл әлдеқайда қауіпсіз.

Ескерту: Желіаралық экрандар бұл параметрлерді тек WindowsSocket арқылы жұмыс істейтін программалар үшін қолдана алады. Белгілі бір программаны құрудың ерекшеліктері алдын-ала белгілі болмағандықтан, ережені жасағаннан кейін оның жұмысын тексеріп, егер қателер болса оны протокол (порт) негізінде орнату керек.

Егер сіз трафикті бастапқы және тағайындалған адрестер негізінде сүзгіден өткізгіңіз келсе, реттелетін ережені таңдау қажет. Ереже бір ғана адресті немесе IP адрес ауқымын да анықтауға мүмкіндік береді. Сонымен қатар, сіз ережеде компьютерлер тобын функционалдық мақсатына сәйкес көрсете аласыз: WINS, DHCP немесе DNS серверлері, шлюз немесе жергілікті ішкі желі. Бұл тапсырма осы рөлдердің желідегі басқа компьютерлерге берілуін ескере отырып, ережелерді дәл баптауға мүмкіндік береді.

Программалық кешендер

Нарықта желіаралық экран ұсыныстары өте көп. Әкімшінің көп немесе аз функционалдығы бар шешімдерді таңдау мүмкіндігі бар. Қалай болғанда да, әкімші шешім қабылдамас бұрын нені қалайтынын және қанша шығын шығатынын мұқият өлшеп алуы керек.

Интернетте жеке компьютерлерді қорғауға арналған көптеген программалар бар. Мысалы, AtGuard, BlackICEDefender, Jammer, KerioPersonalFirewall, OutpostFirewall, SygatePersonalFirewall, Tinypersonalfirewall, ZoneAlarm және т.б. жеке желіаралық экрандарды айтуға болады. Бұл өнімдердің кейбірі коммерциялық программалар, ал кейбірінің тегін пайдалануға болатын нұсқалары бар.

Әдетте, мұндай программалар трафикті бұғаттау мүмкіндіктерін қосымша қызметтермен біріктіреді: мысалы, қалқымалы терезелерге тыйым салу, жарнамалық баннерлерді кесу, қоңырау шалу қосымшасы бойынша сүзгілеу және т.б. көбінесе программаларда тәжірибесі жоқ пайдаланушыға қорғауды дәл орнатуға мүмкіндік беретін оқыту режимі бар. Бұл режимде программа Интернетке ақпарат берудің барлық әрекеттерін хабарлап отырады. Пайдаланушы желіаралық экран ұсынған ақпаратты талдай отырып, ақпарат беруді толық немесе бір реттік, тұрақты бұғаттау туралы шешім қабылдайды. Осылайша, оқытудың нәтижесінде пайдаланушы Интернетке қосылудың конфигурациясын жасай алады.

Кәсіпорын деңгейінде қолдануға арналған өнімдер (Microsoft ForefrontThreatManagementGateway, CheckPoint, TrendMicroInternetGateway және т.б.) әдетте кешенді болып келеді: олардың көмегімен ережелер жасауға, контентті сүзгілеуге, белгілі бір типтегі шабуылдардың алдын алуға және т.б. іске асыруға болады.

Пакеттерді операциялық жүйе құралдарымен сүзгілеу

Windows-те пакеттерді сүзу мүмкіндіктері қарастырылған. Мысалы, сүзгілерді қолдана отырып, мамандандырылған серверді (пошта немесе ұқсас) пакеттерді белгілі бір құрылғылардан тек белгілі бір портқа жіберуге мүмкіндік беру арқылы қорғау оңай.

IPSec саясатының сүзгілерін орнату арқылы белгілі бір желілік түйіндерге трафикке тыйым салатын немесе рұқсат ететін ережелер жасау оңай (сурет. 5.6). Бұл жағдайда IPSec саясатын топтық саясат арқылы желілік компьютерлерге таратуға болады. Осылайша, тұрақты құралдармен сіз жүйенің қауіпсіздік деңгейін тез көтеру құралын жасай аласыз: желінің өзара әрекеттесуін барынша азайтатын IPSec топтық саясатын алдын-ала жасап, оларды вирустық шабуыл немесе желіге кіру белгілері болған жағдайда қосу жеткілікті.

Сурет 5.6.

IPSec сүзгілері жүйенің белгілі бір трафигін беру рұқсаттарын дәл баптауға мүмкіндік береді

Желіаралық экран параметрлерін топтық саясатты қолдану арқылы баптау

Соңғы қауіпсіздік жаңартулары бар Windows нұсқаларында желіаралық экран әдеттегідей бірден қосылады. Бұл жағдайда белгілі бір «орташа» нұсқа үшін оңтайлы параметрлер қолданылады: қорғаныс белсенді, бірақ компьютерді жергілікті желіде жұмыс істеуге мүмкіндік беретін ерекшеліктер бар. Бұл, бір жағынан, кеңейтілген басқару жүйелері бар жергілікті желіде ыңғайсыз: желіаралық экран (ЖАЭ) мұндай программалардың компьютерлерге кіруіне тосқауыл қояды, ал екінші жағынан, бұл жалпы желілерде тиісті деңгейде қорғанысты қамтамасыз етпейді. Сондықтан кіріктірілген Windows брандмауэрлері топтық саясат көмегімен орталықтандырылған орнатуды қажет етеді.

Желіаралық экранның топтық саясаты

Windows желіаралық экранының топтық саясат параметрлері келесі жолда орналасқан: компьютер конфигурациясы / әкімшілік шаблондар | желі | желілік қосылымдар / Windows брандмауэрі (сурет. 5.7). Параметрлер егжей-тегжейлі

түсіндірілген, сондықтан біз тек конфигурацияның негізгі сәттеріне назар аударамыз.

Сурет 5.7.
Топтық саясат арқылы ЖАЭ параметрлерін баптау

Саясатта екі контейнер бар: домен профилі және стандартты профиль. Домен профилінің параметрлері компьютер домен желісінде жұмыс істеген жағдайда қолданылады (домен құрамындағы жұмыс желілік адрес параметрлері және домен бақылаушысының қолжетімділігі бойынша анықталады). Егер компьютер, мысалы, ноутбук, басқа желіге қосылған болса, онда желіаралық экран параметрлері стандартты профиль контейнеріндегі параметрлерге сәйкес орындалады.

Екі жағдайда да қолдануға қандай параметрлерді ұсынуға болады? Біріншіден, ең қауіпсіз нұсқа – желіаралық экранды доменде де, жалпы желіде де пайдалану. Екіншіден, қорғауды алып тастау саясаты анықталуы керек. Доменде жұмыс істеу кезінде, әрине, жергілікті желідегі жұмысқа қатысты ережелер енгізілуі керек. Сонымен қатар, сіз кәсіпорында қолданылатын басқару программалары үшін ерекшеліктер жасап, оларды топтық саясатта көрсетуіңіз керек. Мысалы, егер сіз корпоративті антивирустық программаны қолдансаңыз, онда ол пайдаланатын порттардағы компьютерлерге кіруге рұқсат беруіңіз керек (мысалы, Symantec антивирусы үшін пайдаланылатын порттар: http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2005033011582148?OpenDocument&src=ent_hot&dtype=corp&seg=ent&prod=Symantec%20Client% 20Firewall&ver=8.0&tpre=).

Ал егер кәсіпорында қашықтан мониторинг жүйесі енгізілген болса, онда осы программа үшін порттар ашылуы немесе қашықтағы консоль арқылы басқару мүмкіндігі үшін қашықтан басқару үшін ерекше жағдайларды шешу опциясы қосылуы тиіс. Әр нақты жағдайда мұндай ерекшеліктердің тізімі жеке болып табылады және олардың саны кем дегенде ақылға қонымды болуы керек.

Стандартты профиль үшін ереже желіаралық экрандағы барлық ерекшеліктерді пайдалануға тыйым салуы керек, өйткені бұл опция қоғамдық желі үшін ең қауіпсіз болып табылады.

5.1.-кестеде. Windows желіаралық экранына арналған топтық саясат параметрлерін баптау мүмкіндіктері берілген.

кесте 5.1.
Рекомендуемые параметры настройки МСЭ

Параметр	Профиль үшін ұсынылады	
	домен	стандарттар
Барлық желілік қосылымдарды қорғау	қосылған	қосылған
Ерекшеліктерге рұқсат берілмейді	рұқсат етілмеген	Қосылған және пайдаланылған программалар үшін крұқсат етілген ерекшеліктер
Программалар үшін ерекшеліктерге рұқсат беру	Қосылған және пайдаланылған программалар үшін рұқсат етілген ерекшеліктер	Қосылған және пайдаланылған программалар үшін рұқсат етілген ерекшеліктер
Программалар үшін жергілікті ерекшеліктерге рұқсат беру	ажыратылған	ажыратылған
Қашықтан басқару үшін ерекшеліктерге рұқсат беру	ажыратылған	ажыратылған
Файл мен принтерді бөлісу үшін ерекшеліктерге рұқсат беру	ажыратылған	ажыратылған
ICMP ерекшеліктеріне рұқсат беру	ажыратылған	ажыратылған
Қашықтағы жұмыс үстелі үшін ерекшеліктерге рұқсат беру	қосылған	қосылған
UPnP инфрақұрылымы үшін ерекшеліктерге рұқсат беру	ажыратылған	ажыратылған
Хабарландыруларды өшіру	ажыратылған	ажыратылған
Журнал жүргізуге рұқсат беру	көрсетілмеген	көрсетілмеген
Көпадресті немесе кеңінен хабар тарату сұрауларына бір реттік жауаптар үшін тыйым салу	қосулы	қосулы
Порт үшін ерекшеліктерге	ажыратылған	ажыратылған

рұқсат беру		
Жергілікті порт үшін ерекшеліктерге рұқсат беру	ажыратылған	ажыратылған

Linux желіаралық экраны

Linux операциялық жүйелерінде желілік трафикті басқарудың дамыған функциялары бар. Ең көп қолданылатыны iptables желіаралық экраны. Программа пакеттерді сүзу параметрлерін Windows-тағы желіаралық экранға қарағанда дәлірек жасауға мүмкіндік береді. Себебі, Linux-та Windows пайдаланушыларына қолжетімді емес, трафикті басқару мүмкіндігі төмен.

Іске қосу параметрлері

Iptables желіаралық экраны барлық заманауи Linux шығарылымдарында қамтылған. Әдетте, амалдық жүйені орнату кезінде әдепкі желіаралық экранды пайдаланғыңыз келе ме, жоқ па деген сұрақ туындайды. Таңдауыңызға байланысты программа іске қосылады немесе өшіріледі. Брандмауэр программасының жұмыс істейтінін немесе жұмыс істемейтінін білу үшін PS-a командасымен процестер тізімін көрсету және оны grep командасымен қызмет атауы бойынша сүзу жеткілікті. Бұл жағдайда пакеттік сүзу ережелерінің жиынтығы компьютер ресурстарына сырттан кіруге тыйым салады және жергілікті желідегі кейбір функцияларды шектейді.

RedHat-та желіаралық экранды іске қосу келесі команданы орындағанда жүзеге асырылуы мүмкін: /sbin/serviceiptablesstart

Демонды тоқтату үшін параметр ретінде stop-ты, қайта іске қосу үшін (конфигурацияны өңдегеннен кейін қажет) — restart-ты көрсету қажет.

Желіаралық экран программасын автоматты түрде іске қосу үшін жүйені әр іске қосу кезінде келесі команданы орындау жеткілікті: /sbin/chkconfig —level 345 iptables on

> Ескерту: Linux-те бірнеше жүктеу параметрлері (деңгейлері) бар. Олар жүйенің бір қолданушы режимінде іске қосыла ма, жоқ па, графикалық ортаны жүктеу қажет пе, жоқ па екенін анықтайды. Қалыпты жұмыс істеуі үшін 3 және 5 деңгейлер сәйкес келеді; олардың арасындағы айырмашылық 3-деңгейде графикалық ішкі жүйенің жүктелмейтіндігінде.
>
> Ескерту: Пайдаланылған дистрибутвке байланысты сіз қызметтерді арнайы утилиталармен орната аласыз. Мысалы, (сурет 5.8) RedHat-да ntsysv утилитасымен қызметті іске қосу параметрі ұсынылған.

Сурет 5.8.

Мәтіндік режимде жұмыс істейтін қызмет параметрлерін теңшеу утилитасы

Ubuntu-да iptables қолдану

Ubuntu-көптеген вендорлар қолдайтын Linux клондарының ең танымалының бірі. Ubuntu-да желіаралық экранның жеңілдетілген нұсқасы қолданылады, сондықтан жүйеде iptables программасын іске қосу сценарийі жоқ, тиісті параметрлер файлдары жоқ. Iptables пайдалану үшін арнайы қадамдарды орындау керек:

1. iptables командасын пайдаланып, трафикті сүзудің қажетті ережелерін жасаңыз;
2. Параметрлерді iptables-save командасы арқылы файлға экспорттаңыз;
3. Ubuntu әр іске қосылған сайын осы файлдан параметрлерді автоматты түрде жүктеуді реттеңіз.

Автоматты жүктеудің ең оңай жолы - желілік интерфейсті конфигурациялау опциялары, желілік интерфейсті қосу және өшіру алдында жасалатын қадамдарды сипаттайтын жолдар қосу. Ол үшін қолданыстағы ережелерді конфигурациялау және сақтау жеткілікті (мысалы, sudobash-c «iptables-save>/etc/iptables.rules» командасымен), содан кейін /etc/network/interfaces файлын өңдеу үшін ашып, желілік интерфейсті сипаттайтын параметрлер блогының соңына келесі жолдарды қосыңыз: pre-upiptables-restore < /etc/iptables.rules
post-down iptables-save -c > /etc/iptables.rules2

Бұл командалар желілік интерфейсті қосқан және өшірген сайын орындалады және бұрын жасалған ережелерді белсендіреді (қолданыстағы параметрлерді файлға сақтаңыз).

/Etc/iptables.rules файлының бар екенін жүйені қайта жүктеместен бұрын тексеріп алыңыз, әйтпесе желілік интерфейс қосылмайды.

Iptables графикалық басқару программалары

Желіаралық экранды дәл баптау үшін сізге команда беру жолына кіріп, параметрлердің толық жиынтығымен тиісті ережелерді қосу қажет - бұл ереже

оған қолданылуы үшін пакет орындалуы керек жағдайлар. Linux-тің жаңа пайдаланушысы үшін бұл айтарлықтай қиындық тудыруы мүмкін.

Көп жағдайда желіде Қауіпсіз жұмыстың қажетті деңгейін қамтамасыз ету үшін стандартты шектеулерді қолдану жеткілікті. Мұндай жағдайларда брандмауэрді конфигурациялау үшін графикалық утилиталарды қолдануды ұсынамыз. Оларды Surceforge.net сайтындағы тегін программалардың ішінен оңай табуға болады. Мысал ретінде, (сурет 5.9) осындай программалардың бірінің интерфейсі көрсетілген.

Сурет 5.9.
Желіаралық экран параметрлерін графикалық баптау

Суретте FireStarter программасының экрандары көрсетілген. Оның көмегімен желіаралық экранның жиі қолданылатын параметрлерін графикалық режимде баптау оңай. 5.9. суретте – қызметті жариялау ережелерін орнату терезесі көрсетілген, ал 5.9,б суретте – трафикке басымдық беру мүмкіндіктерін қосу көрсетілген. Программа желіаралық экран оқиғаларын бақылауға, кіріс және шығыс трафик ережелерін жасауға, қосылымды бөлісу режимін баптауға және т.б. мүмкіндік береді.

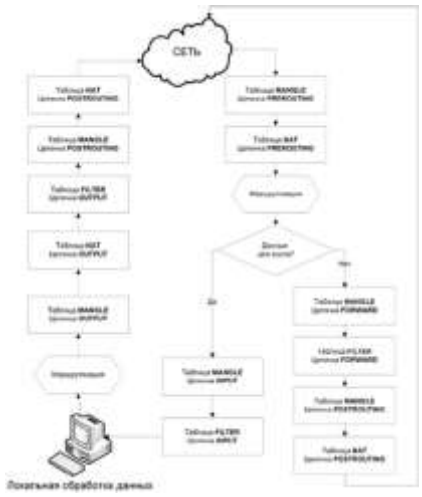
Iptables жұмысының принциптері

Кез-келген пакет компьютердің әр желілік интерфейсінің кейбір шарттарына қаншалықты сәйкес келетінін анықтау үшін бірнеше рет талданады. Шарттар қанағаттандырылған кезде пакетке тиісті ереже қолданылады және осы кезеңде одан әрі талдау жүргізілмейді. Егер ережелердің ешқайсысында пакетке сәйкес шарттар болмаса, оған әдепкі ережелер қолданылады. Мұндай ережелер жиынтығы кесте деп аталады

Ереженің үш кестесі бар: filter – негізгі кесте, nat – жаңа қосылымды құратын пакеттер үшін қолданылады (пакеттің мақсаты мен адрестерді өзгертуге болады) және mangle – пакеттердің арнайы түрі үшін қолданылады.

5.10 суретте пакетті қабылдау немесе жіберу кезінде талдау реттілігі көрсетілген. Желіаралық экранды орнату үшін пакет жолы бойынша ереже жасау керек. Мысалы, кіріс трафикті сүзу үшін шығыс – OUPTUT тізбегінде ереже жасау керек. FORWARD тізбегінде жүйемен (сервер арқылы өтетін)

жіберілетін трафикті сүзуге болады. PREROUTING сыртқы трафикті жарияланған ішкі ресурсқа және т.б. бағыттау үшін қолданылады.



Сурет 5.10.
Iptables сүзгілеріндегі деректер пакетін талдау реттілігі

Ескерту: Ережелер олардың тізімі бойынша орындалады. Сондықтан олардың реттілігіне назар аударыңыз. (A командасы ережені тізімнің соңына қосады, I <нөмір> - тізімнің көрсетілген позициясына орналастырады).

Сүзгінің шарттарына сәйкес келетін пакеттерде бірнеше әрекеттерді жасауға болады: оларды өткізіп жіберуге (ACCEPT), дереккөзге деректерді жіберу қателігі туралы ескерте отырып, жоюға (REJECT) немесе үнсіз жойып жіберуге (DROP). Сондай-ақ, баптау және бапталатын өңдеу параметрін қолдану мүмкіндігі бар (QUEUE).

Желіаралық экран ережелерін жасау

Жалпы алғанда, желіаралық экран ережелерін өңдеу командасы келесідей:

```
iptables [-t table-name ] command chain-name parameter-1 option-1 parameter-n
option-n
```

Table-name параметрі пайдаланылған кестені таңдауға мүмкіндік береді. Command орындалатын әрекетті анықтайды: ережені қосу немесе алып тастау. Chain-name –сәйкес келетін ереженің атауы. Одан кейін parameter-n option-n жұптарының жиынтығы берілген, олар іс жүзінде программаның нақты әрекеттерін анықтайды.

Команда параметрлерінің сипаттамаларын Интернеттен оңай табуға болады. Толығырақ iptables орнату процесі келесі оқулықта келтірілген: *(Практическое руководство системного администратора. - СПб.: БХВ-Петербург, 2010.-464 с.)*. Ал, мұнда біз Интернетте жұмыс істеу үшін Linux жүйесін минималды орнатуды орындайтын командалардың мысалын қысқаша қарастырамыз:

```
iptables -A INPUT -i eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0 -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i eth1 -p tcp -m tcp --dport 22 -j ACCEPT
iptables -P INPUT DROP
iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to-source xxx.xxx.xxx.xxx
```

Бірінші ереже сыртқы интерфейске (eth1) шығыс трафикке жауап беретін пакеттерді қабылдауға мүмкіндік береді (RELATED және ESTABLISHED күйі.

Екінші және үшінші ережелер ішкі және жергілікті интерфейстердегі барлық кіріс трафикке мүмкіндік береді.

Төртінші ереже ssh протоколы арқылы басқару үшін Интернеттен серверге қосылуға мүмкіндік береді (іс жүзінде барлық жүйелерден емес, тек нақты адрестерден қатынасуға рұқсат берген жөн). Бесінші ереже әдепкі саясатты DROP-қа ауыстырады: жоғарыда көрсетілген тізімнен басқа пакеттерге рұқсат етілмейді.

Соңғы ереже сыртқы жүйелермен алмасу өтетін адресті нақты көрсететін алдыңғы бетке арналған NAT режимін қамтиды.

Интернетке кіру аутентификациясы

Кіріктірілген Linux желіаралық экранды сүзу ережелерін өте дәл баптауға мүмкіндік береді, бірақ олар сессия деңгейінде жұмыс істемейді. Сондықтан, егер мұндай қорғау корпоративті ортада қолданған жағдайда, кибершабуылшылар қорғанысты айналып өтуі үшін басқа компьютерлердің адрестерін иемденуге мүмкіндік алады. Бұл жағдайда қабылданатын шешім – Интернетке қол жеткізудің кез-келген әрекетін аутентификациялау.

Мұндай желіаралық экрандарды, әдетте, Windows жүйелері үшін коммерциялық клиенттер ұсынады. Мұндай өнімді сатып алуға болады, бірақ басқа да шешімдер бар.

Олардың бірі желіаралық экрандағы ортақ ресурсқа қосылатын домен пайдаланушысына негізделген (бұл байланыс доменге кіру сценарийлерінде оңай конфигурациялануы мүмкін). Байланыстың болуы және оның параметрлері сұранысты өңдеу сценарийлерінде қолданылады.

Тағы бір тәсіл – желіаралық экранға VPN қосу арқылы Интернетке қолжетімділікті қамтамасыз ету. Мұндай тәсілді кішігірім Интернет-провайдерлер жиі қолданады, өйткені бұл әр клиенттің трафик көлемін есептеуді жеңілдетеді.