А. И. БАРАНЧИКОВ, П. А. БАРАНЧИКОВ,

А.Ю. ГРОМОВ

ЖЕЛІЛІК ӘКІМШІЛІКТЕНДІРУДІ ҰЙЫМДАСТЫРУ

ОҚУЛЫҚ

«Компьютерлік желілер» мамандығы бойынша орта кәсіптік білім беру бағдарламаларын жүзеге асыратын білім беру мекемелерінің оқу процесінде қолдануына арналған оқулық ретінде «Федералдық білім беруді дамыту институты» федералдық мемлекеттік автономиялық мекемесімен ұсынылған.

2015 жылғы 12 қарашадағы «БДФИ» ФМАМ рецензиясының тіркеу нөмірі 487

ACADEMIA
Мәскеу
«Академия» баспа орталығы
2016

ӘОЖ 004.7(075.32)
КБЖ 32.973.202ші723
Б243

Бұл кітап Қазақстан Республикасының Білім және ғылым министрлігі және «Кәсіпқор» холдингі» КЕАҚ арасында жасалған шартқа сәйкес «ТжКБ жүйесі үшін шетел әдебиетін сатып алуды және аударуды ұйымдастыру жөніндегі қызметтер» мемлекеттік тапсырмасын орындау аясында қазақ тіліне аударылды. Аталған кітаптың орыс тіліндегі нұсқасы Ресей Федерациясының білім беру үдерісіне қойылатын талаптардың ескерілуімен жасалды.

Қазақстан Республикасының техникалық және кәсіптік білім беру жүйесіндегі білім беру ұйымдарының осы жағдайды ескеруі және оқу үдерісінде мазмұнды бөлімді (технология, материалдар және қажетті ақпарат) қолдануы қажет.

Аударманы «Delta Consulting Group» ЖШС жүзеге асырды, заңды мекенжайы: Астана қ., Иманов көш., 19, «Алма-Ата» БО, 809С , телефоны: 8 (7172) 78 79 29, эл. поштасы: info@dcg.kz

Пікір беруші —
С.А.Есенин атындағы Рязань мемлекеттік университетінің Информатика және есептеуіш техника кафедрасының профессоры, техн. ғыл. Докторы, профессор *В. Н. Ручкин*

Баранчиков А. И.

Б243 Желілік әкімшіліктендіруді ұйымдастыру: орта кәсіптік білім беру студ. арналған оқулық / А. И. Баранчиков, П. А. Баранчиков, А. Ю. Громов. — М. : «Академия» баспа орталығы, 2016. — 320 б.

ISBN 978-601-333-251-2 (каз.)
ISBN 978-5-4468-2343-7 (рус.)

Оқулық «Желілік әкімшіліктендіруді ұйымдастыру» КС.02 кәсіби модулін меңгеру үшін «Компьютерлік желілер» мамандығы бойынша Федералдық мемлекеттік білім беру стандартының талаптарына сай жазылған.

Жергілікті есептеуіш желілерді әкімшіліктендіру мәселелері және ықтимал ақауларды жою жөніндегі шаралар қарастырылған.

Орта кәсіптік білім беру студенттеріне арналған.

ӘОЖ 004.7(075.32)
КБЖ 32.973.202ші723

ISBN 978-601-333-251-2 (каз.)
ISBN 978-5-4468-2343-7 (рус.)

Құрметті оқырман!

Осы оқулық «Компьютерлік желілер» мамандығына арналғаноқу-әдістемелік жинақтың бір бөлігі болып табылады.

Оқулық «Желілік әкімшіліктендіруді ұйымдастыру» КМ.02 кәсіби модулін меңгеруге арналған.

Жаңа заманның оқу-әдістемелік жинақтарының ішіне жалпы білім беру және жалпы кәсіптік пәндер мен кәсіптік модульдерді меңгеруді қамтамасыз етуге мүмкіндік беретін дәстүрлі және инновациялық оқу материалдары кіреді. Әрбір жинақтың ішінде жалпы және кәсіптік құзыретті меңгеру үшін қажетті, соның ішінде, жұмыс беруші талаптарын ескере отырып, білім беру және бақылау құралдары, оқулықтар мен оқу құралдары бар.

Оқу басылымдары электронды оқыту ресурстарымен толықтырылады. Электронды ресурстардың құрамында интерактивті жаттығулары бар теориялық және тәжірибелік модульдер, мультимедиялық нысандар, Интернеттегі қосымша материалдар мен ресурстарға сілтемелер бар. Олардың ішіне оқу процесінің негізгі параметрлері, яғни, жұмыс уақыты, бақылау және тәжірибелік тапсырмаларды орындау нәтижелері жазылатын электронды журнал мен терминологиялық журнал кіріктірілген. Электронды ресурстар оқу процесіне оңай енгізіледі және түрлі оқу бағдарламаларына бейімделуі мүмкін.

Алғы сөз

Орта кәсіптік білім берудің «Компьютерлік желілер» мамандығы бойынша Федералдық мемлекеттік білім беру стандартына сәйкес «Желілік әкімшіліктендіруді ұйымдастыру» КМ.02 кәсіптік модулін меңгеру нәтижесінде білім алушы мыналарды:

білуі керек:

- компьютерлік желілерді әкімшіліктендірудің негізгі бағыттарын;
- серверлер типтерін, «клиент-сервер» технологиясын;
- серверді орнату және басқару әдістерін;
- утилиталар, қызметтер, серверді қашықтықтан басқаруды;
- Web-те жұмыс жасау кезіндегі құпиялылық пен қауіпсіздікті, авторизация хаттамаларын, қауіпсіздік технологияларын;
- кластерлерді пайдалануды;
- түрлі операциялық жүйелердің өзара әрекеттестігін;
- қызмет көрсету міндетерінің авторизациясын;
- өнімділік мониторингі мен баптауларын;
- есептік құжаттаманы жүргізу технологиясын;
- желілік технологияларды қамсыздандыру бағдарламасының жіктелімін және оны қолдану аясын;
- бағдарламалық қамсыздандыруды лицензиялауды;
- бағдарламалық қамсыздандыруды пайдалану әдісі мен орнына қарамастан, оның құнын бағалауды;

орындай алуы керек:

- жергілікті есептеуіш желілерді әкімшіліктендіру;
- ықтимал ақауларды жою бойынша шаралар қабылдауды;
- ақпараттық жүйе орнатуды;
- жекелеген пайдаланушылар мен пайдаланушылар тобының есеп жазбасын құру және конфигурациялауды;
- доменге қосылуды тіркеуді, есептік құжаттаманы жүргізуді;
- желілік инфрақұрылымды лицензиялық бағдарламалық қамсыздандырудың құнын есептеуді;
- вирусқа қарсы бағдарламалық қамсыздандыруды, мәліметтер базасының бағдарламалық қамсыздандыруын, мониторингтің бағдарламалық қамсыздандыруын ортануды және конфигурациялауды;
- операциялық жүйе құралдарымен Интернетке қосылу кезінде қорғанышты қамтамасыз етуді;

мына практикалық тәжірибесі болуы керек:

- ақпаратты қауіпсіз жолдау үшін сервер мен жұмыс станцияларын

баптаулар бойынша;

- Web-серверді орнатулар бойынша;
- жергілікті және жаһандық желілерге қолжетімділікті ұйымдастыру, пошталық сервер, SQL-сервер және т.б. қолдануды сүйемелдеу және бақылау бойынша;
- желілік инфрақұрылымды лицензиялық бағдарламалық қамсыздандырудың құнын есептеу бойынша;
- компьютерлік желілердің бағдарламалық-техникалық құралдарын пайдалану және олардың қызмет етуін талдауға арналған мәліметтер жинау бойынша.

Кіріспеде осы міндеттерді шешу барысында назар аударуды қажет ететін негізгі басты кезеңдері қарастырылған, желілік әкімшіліктендіруді ұйымдастыруға арналған әдістер сипатталған.

I бөлімде компьютерлік желілерді бағдарламалық қамсыздандыруды пайдалану мәселелері қарастырылған. Бұл тарау екі бөлімнен тұрады.

1-тарау Web-серверді орнатуға арналған және келесі мәселелерді қамтиды:

- аппараттық бөлікті таңдау, соның ішінде, жедел жады мен дисктерді;
- Web-серверді конфигурациялау, соның ішінде, TCP-порттардың ерекшеліктерін, қорғаныш жүйесімен өзара әрекеттестік, сервердің түпкі каталогы, өнімділікті ұлғайту, ресурстар жоғалтуды шектеу, серверлер саны, индекстер құру және (немесе) индекстер бойынша іздеу, уақыт бойынша кейбір қосылуларды шектеу, директивалардың әрекет ету аймағын шектеу;
-
- OCLinux, Windowsи MaxOC басқаруындағы серверді іске қосу, қайта қосу және тоқтату;
- пайдаланушылардың үй парақшалары, IP-мекенжайлары және порттары қарастырылатын бірнеше Web-тораптардың хостингі, атауы бойынша виртуалды хостинг, IP-мекенжайы бойынша виртуалды хостинг;
- қателіктерді, сайттарды тіркеу, тіркеу және мәліметтер алмасу журналдары, сондай-ақ, *mod_status* мәртебе модулінің және іске қосылу проблемалары мәселелерін қарастыратындарды тіркеу және мониторинг;
- қауіпсіздік, соның ішінде, каталогтар қауіпсіздігін қоса алғанда, автоматты индекстеуді сөндіру, пайдаланушылар құқықтарын, сәйкестендіру негіздерін, пайдаланушы бойынша сәйкестендіруді сөндіру, топтық қолжетімділікті бақылау, әрекет етуші пайдаланушыларды анықтау, ашық кілтпен шифрлау және сертификаттау;
- ресуртар тұтынуды басқару және процестер арасындағы өзара

әрекеттестік, сервер жағындағы кіріктірмелер, кіріктірмелер листингі, CGI интерфейсі қарастырылатын үдемелі Web-парақшалар;

-
- MySQL МББЖ және Oracle МББЖ басқаруындағы базалармен мәліметтер алмасу мысалында мәліметтер базаларымен өзара әрекеттестік;
- mod_rewrite модулі, мекенжайды қайта тағайындау, үлгі бойынша URL-ді қайта жазу, файлдарды реттеу, негізгі каталогты тағайындау, мұралау, тіркеуге қатысты мекенжайды қайта тағайындау.

2- тарау брандмауэр орнатуы және параметрлеріне арналған. Онда мыналар қарастырылған:

- ядроны баптау, орнатуға арналған пакетті жинақтау және пакетті орнату кіретін брандмауэр орнату;
- кестелер мен тізбектерді өту тәртібі (жалпы ережелер, Mangle, Nat және Filter кестелері);
- жол тартқыш кестесіне, пайдаланушы кеңістігіндегі күйлерге, TCP-, UDP- және ICMP-қосылыстарға негізделетін күйлерді анықтау механизмі, әдепкі қалпы бойынша тәртібі және кешенді хаттамалардың жол тартуы;
- ережелердің үлкен жинағын сақтау және қалпына келтіру, iptables-save, iptables-restore артықшылықтары мен кемшіліктері;
- ережелерді құру қағидалары – кестелер, пәрмендер, өлшемдер, жалпы өлшемдер, жасырын өлшемдер, айқын өлшемдер, «қоқыс» өлшемдері (UncleanMatch);
- (ACCEPT, DNAT, DROP, LOG, MARK, MASQUERADE, MIRROR, QUEUE, REDIRECT, REJECT, RETURN, SNAT, TOS, TTL, ULOG) әрекеттері мен ауысулар.

II тарауда компьютерлік желілерге қызмет көрсету және әкімшіліктендіру мәселелері қарастырылған.

3- тарау сервер баптаулары мен ақпаратты қауіпсіз жолдауға арналған жұмыс станцияларын қамтиды. Оның аясында келесі мәселелер қарастырылады:

- DCHPServer қызметінің баптаулары, соның ішінде, IP-мекенжайлардың диапазондарын құруды, резервтелген IP-мекенжайларды конфигурациялауды, DHCP-опциялардың баптауларын қоса алғанда;
- DNSServer қызметінің баптаулары (аумақтар құру, DNSServer қызметі клиентінің баптаулары, DNSServer қызметін қолданумен хосттар атауларына рұқсат беру процесінің баптаулары);
- доменнің ақпараттық жүйесінің баптаулары (доменді әкімшіліктендіру құралдарын орнату және конфигурациялау, пайдаланушының есеп жазбаларын құру, топтар құру, топтағы мүшелікті басқару);
- доменнің топтық саясаттарының баптаулары (топтық саясаттарды

қолдануды басқару, қауіпсіздік үлгісін құру және оны топтық саясатпен бірге қолдану);

- ақпаратты қауіпсіз жолдауды конфигурациялау (IPsec хаттамаларын қолдану, шифрлеуші файл жүйесінің конфигурациялануы, RADIUS қызметінің көмегімен аутентификациялау).

4- тарау жергілікті және жаһандық желілерге қолжетімділікті ұйымдастырудың келесі мәселелерін қозғайды:

- бағдарлау жұмысының логикалары, статикалық және үдемелі бағдарлау, статикалық және үдемелі бағдарлау баптаулары қарастырылатын бағдарлаудың негізгі қағидалары;
- ішіне Wi-Fi жабдығының (қолжетімділік нүктелері) баптаулары, клиенттер машинасындағы баптаулар және қосылу профилін құру кіретін сымсыз қосылу бойынша желілерге қолжетімділікті ұйымдастыру;
- кэштеуші прокси-серверді ұйымдастыру, оның аясында AccessControlList баптаулары, пайдаланушылардың аутентификацияларын қолдану және прокси-серверлердің сатыларын пайдаланы ерекшелігі меңгеріледі;
- құрамына брандмауэр (Firewall), желілік мекенжайларды тарату жүйелерін (NAT) және әділ проксилеу (transparentproxy) баптаулары кіретін жаһандық желілерге қолжетімділік кезіндегі қорғанышты қамтамасыз ету.

5- тарау Web-серверді, файлдық серверді, пошталық серверді, SQL-серверді сүйемелдеу және оларды қолдануды бақылауға арналған.

Онда мыналар қарастырылған:

- Web-серверді сүйемелдеу және бақылау (сервер конфигурациясын бақылау, серверге қолжетімділікті шектеу, мәліметтер жолдауды оңтайландыру, модульдер мен сервер қызметтерін жаңартау);
- файлдық серверді сүйемелдеу және бақылау (сервер конфигурациясын бақылау, пайдаланушылардың ресурстарға қолжетімділік құқықтарының баптаулары, сервер қызметтерін жаңарту);
- пошталық серверді сүйемелдеу және бақылау (пошта жолдау және қабылдауды бақылау, пайдаланушылардың пошталық акаунттарға қолжетімділік құқықтарының баптаулары, сервер қызметтерін жаңарту);
- SQL-серверді сүйемелдеу және бақылау (сервер конфигурациясын бақылау, резервтік көшірмелеу және мәліметтер базасын қалпына келтіру, пайдаланушылардың мәліметтер базасына қолжетімділік құқықтарының баптаулары, сервер қызметтерін жаңарту);
- SQL-сервері қызметтерін (сервер қызметтерінің өнімділігін, SQL-сервері қызметтерімен мәліметтер алмасуды және қызметтердің жадыны қолдануын) оңтайландыру.

Оқулық практикалық бағыттамаға ие. Күнделікті жұмыс кезінде туындайтын желілік әкімшіліктендіру міндеттерін шешуге байланысты практикалық мәселелерді шешуге зор көңіл бөлінеді.

Авторлар оқулықты жазуға көмектескен ұстаздар мен студенттерге және материалдары қолданылған барлық авторларға үлкен алғыс білдіреді және мәтін ішінде мұндай қолданудың барлығына сілтеме жасау мүмкіндігі болмағаны үшін кешірім өтінеді.

Кіріспе

1980 жылдардың басында компьютерлерді ортақ файлдарды, сервистерді және ресурстарды қолдану үшін желіде біріктіре бастады. Кейінірек бұл желілер едәуір ірі және күрделі бола бастады. Оларды басқару жеке маңызды міндет болып табылды.

Желіні басқару берілген бағдарлама бойынша оның жұмысын ұйымдастыруда болып табылады.

OSI моделі көзқарасы бойынша желіні басқару конфигурацияны, бас тарту, трафикті және есепті басқаруға бөлінеді.

Басқарудың классикалық әдістері компьютерлік желінің басқару жүйесіне білгілі бір оқиғалар орын алған кезде белгілі бір әрекеттерді орындауды тағайындайтын ережелерді қолданады.

Шағын желілер үшін жеткілікті ережелер негізіндегі басқару әдіснамасы ірі желілерде үлкен кедергілерге ұшырайды, себебі, үлкен есептеуіш ортаның жұмыс істеуі параметрлердің ораан зор санымен сипатталады.

Корпоративтік желі (enterprisenetwork) немесе кәсіпорын масштабының желісінде бірнеше жергілікті есептеуіш желі бар. Ол корпорация филиалдарын біріктіреді және кәсіпорын меншігі болып табылады.

Кейбир негізгі ұғымдарды қарастырып көрейік.

Пайдаланушы/келуші (user; visitor) — оған желіде қолжетімді ақпараттық ресурсты пайдаланушы.

Сервер (server) — клиенттерге желілік сервистерді пайдалануға мүмкіндік ұсынатын компьютер және (немесе) бағдарлама.

Желіні басқару жүйесі (networkmanagementsystem) — желі тораптарының мониторингі және оларды басқару үшін қолданылатын аппараттық және (немесе) бағдарламалық құралдар. Желіні басқару жүйесінің бағдарламалық қамсыздандыруы желілік құрылғыларды іске қосылған және желілік басқарушы платформаға ақпарат жолдайтын агенттерден тұрады.

Желіні басқару платформасы (networkmanagementplatform) — желіні басқаруға арналған бағдарламалар кешені.

Өз қызметтерін тиімді жүзеге асыру үшін компьютерлік желі өз элементтерінің күйлерін бақылауы керек, туындаған проблемаларды анықтауы және шешуі керек, өнімділік талдауын орындауы және желінің дамуын жоспарлауы керек, бұл негізінен, желілерді әкімшіліктендірудің негізгі міндеттері болып табылады.

Оның жұмыс істеуі параметрлерінің пайдаланушылардың сәйкес қажеттіліктеріне жетуі желіні басқару мақсаты болып табылады. Пайдаланушылар қолданбалы бағдарламалық қамсыздандырудың жұмысын желілік трафик сипаттамалары, қолданылатын хаттамалар, белгілі бір типтегі сұраныстарға серверлердің жауап қату уақыты және басқарудың орындалатын сценарийлерінің ерекшеліктері бойынша емес, олардың жұмыс орындарында күн сайын іске қосылатын қосымшалардың іс-әрекеті бойынша бағалайды.

Осылайша, желілік әкімшіліктендірудің басты міндеті – жекелеген ресуртар немесе олардың топтарынан бақылау екпінін ақпараттық технологиялардың негізгі пайдаланушыларының сұраныстарын максималды қанағаттандыруға көшіру үдемелі әімшіліктендіру тұжырымдамасының туындауына ықпал етті.

Бұл әдіс пайдалунышар әрекеттерін талдау құралдарының бар болуын бағамдайды,бұл құралдар жұмыс процесінде туындайтын артықшылықтары мен проблемаларын анықтайды. Алынған нәтижелер әкімшіліктендірудің негізгі нысандары – пайдаланушылар, қосымшалар және желі арасындағы өзара әрекеттестікті белсенді басқаруға арналған бастапқы нүктесі болып қызмет етеді.

Желіні басқарудың біріктірілген жүйесі (IntegratedNetworkManagementSystem — INMS) — желіні басқару, диагностикасы және талдауымен байланысты қызметтерді біріктіретін жүйе.

Әкімшілік механизмдерді дамыту стратегиялық басқаруды орнату, ақпараттық ресурстарға, бағдарламалық-аппараттық құрылғыларға, жүйелер мен кешендерге қолжетімділік пен ақпараттық қамсыздандыру саясатын әзірлеуді білдіреді.

Желі әкімшісінің мақсаттары мен міндеттері. Желі әкімшісі – есептеуіш желінің қалыпты жұмыс істеуіне жауап беретін қызметкер.

Желіні әкімшіліктендіруге келесі міндеттер жатады:

- желіні орнату және баптау;
- оның жұмыс істеу қабілеттілігіне қолдау көрсету;
- негізгі желілік бағдарламалық қамсыздандыруды орнату;
- желі күйінің мониторингі.

Желінің жұмыс істеу қабілеттілігін қамтамасыз ету профилактикалық шараларды жүзеге асыруды да талап етеді. Әкімші пайдаланушылардың рұқсат етілген сұраныстарының қанағаттандырылуын қамтамасыз етуі керек.

Күрделі компьютерлік желілерді әкімшіліктендіру осы процестерді автоматтандырудың жаңа құралдары мен жүйелерін қолданумен жүзеге асырылады.

Желіні басқаруды автоматтандыру. Желілік қызметтер желінің түрлі

абоненттік жүйелерінде орналасқан қолданбалы процестердің байланысын қамтамасыз ететін сервистерді қолданады.

Желіні басқаруды әкімшінің жұмыс орнынан жүзеге асыру қажет. Желіні бір станциядан бақылау қажеттілігі әкімшіліктендірудің түрлі қосымшаларының пайда болуына әсер етті. «Менеджер-агенттер» үлестірілген архитектурасы кеңінен таралды. Бағдарлама-менеджер желінің бөлек құрылғыларын жұмыс істейтін модуль-агенттермен өзара әрекеттесе отырып, басқарушы консольде жұмыс жасайды. Бақыланатын ресурс жұмысының параметрлері туралы мәліметтер жинау, әкімші сұранысы бойынша оның конфигурациясына өзгерістер енгізу, оған ақпарат ұсыну қызметтері агенттерге жүктеледі. Алайда, оны қолдану қызметтік трафик көлемінің ұлғаюына алып келеді.

Үш деңгейлі сызбада басқарушы қызметтерді бір бөлігі нақты желілік тораппен ұсынылады. Бағдарлама-менеджерлер өздеріне тиесілі агенттер арқылы өздерінің құрылғыларының жұмыстарын басқарады және негізгі бағдарлама-менеджерге қатысты агенттер рөлінде болады. Қызметтік трафиктің басым бөлігі жекелеген желілік сегменттерде шектетілген болады.

Желілік әкімшіліктендіру технологияларын дамыту адам рөлін минимумға жеткізуде болып табылады. Желілік әкімшіліктендіру үшін қорғанышты бақылауды, пайдаланушыларды басқаруды, бағдарлауды, ақпаратты резервтік көшірмелеуді және т.б. біріктіруге мүмкіндік беретін бағдарламалық қамсыздандыру құрылады. Бұл жағдайда, желіні әкімшіліктендіру желі әкімшісімен күйге келтірілетін бағдарлама жүзеге асырады. Мұндай шешім әкімшіліктендіру процесін жеңілдетеді.

Көпшілік пайдаланатын ақпараттық жүйелер және орталар. Құрылу қағидалары мен мысалдары. Желі көлемінің ұлғаюы құрылғылар мөлшері мен желі пайдаланушылар санының артуына алып келеді. Мұндай жүйелер мен орталар көпшілік пайдаланатын болып табылады.

Компьютерлік желінің күрделілігі әкімшіні арнайы құрылғылардың көмегімен бірнеше желілерді коммутациялауға арналған құрылғыларды қолдануға мәжбүрлейді: қайталауыштар, көпірлер және бағдарлауыштар.

Қайталауыштар желілік кабель ұзындығын ұлғайтуға мүмкіндік береді.

Көпірлер түрлі желілерді қарапайым желілік құрылымда біріктіруге арналған. Олар жүктемені желінің жекелеген сегменттерінде оқшаулауға мүмкіндік береді.

Бағдарлауыштар — түрлі хаттамаларды айырып танитын және ақпараттар апкетін бір желіден екінші желіге дұрыс бағыттай алатын компьютерлер.

Желі пайдаланушылары — өзінің қолданбалы мәселелерін шешу үшін

желі қызметтерін пайдаланатын тұлға, тұлғалар тобы немесе ұйым.

Желі пайдаланушыларын екі топқа бөлуге болады: әкімшілер және қарапайым пайдаланушылар.

Әкімшілер желіні бағдарламалық және аппараттық қамсыздандыру орнатуларын және бағдарламалық баптауларды жүзеге асырады.

Қарапайым пайдаланушылар вөздерінің практикалық жұмысында желілік ресурстарды және құрылғыларды қолданады.

Бір жұмыс станциясы екіншілеріне қатысты сервер ретінде бола алатын бір дәрежелі желілерге қарағанда, көпшілік пайдаланатын орталардағы жұмыстардың белгіленген сервер базасында «клиент-сервер» архитектурасын пайдаланумен байланысты жұмыстарын атап өтуге болады.

«Клиент-сервер» архитектурасы үлестірілген желілік архитектураның бірінші нұсқасы болып табылды. «Клиент-сервер» қосымшаларында есептеуіш операциялардың және бизнес-логиканың бір бөлігі клиент жағыны көшірілген.

Клиент — серверге сұраныс жолдайтын қосымша. Ол ақпаратты өңдеу, шығаруға және серверге сұраныстар жолдауға жауап береді.

Сервер — клиентке қызмет көрсету қызметтерін орындайтын және жүйе ресурстарын – принтерлерді, мәліметтер базасын, бағдарламаларды, сыртқы жадыны және т.б. үлестіретін ЭЕМ.

Ірі үлестірілген желіні ұйымдастыру кезінде сенімді бағдарлау, ақпарат алмасудың жоғары жылдамдығы және рұқсат етілмеген қолжетімділіктен ақпаратты қорғау қамын ойластыру керек. Сол сияқты, мұндай құрылымның барлық бөліктері үшін бірыңғай ақпараттық қызмет көрсетуді ұйымдастыру керек.

Корпоративтік жүйелердің архитектурасы негізінде жүйені жүзеге асырудың нақты өндірушіге тәуелсіздікті белгілейтін «ашық архитектура» қағидалары жатыр.

Ашық архитектура (openarchitecture) — басқа өндірушілерге олармен өзара әрекеттесуді жүзеге асыруға мүмкіндік беретін жарияланған сипаттамалары бар құрылғының архитектурасы.

Есептеуіш желінің жұмыс істеу қабілеттілігін қолдау – оны әкімшіліктендірудің басты міндеті. Желі әкімшісі үлкен мүмкіндіктерге ие тіркелген пайдаланушы болып табылады. UNIX ОЖ-де оған UID бір нөлдік мән беріледі. Мұндай UID мәні бар пайдаланушы суперпайдаланушы (superuser) деп аталады және root деген атауға ие. Оның жүйеде шектелмеген құқықтары бар, оған толық бақылау жүргізеді және жүйе қауіпсіздігін, оның конфигурациясын, пайдаланушылық есеп жазбаларын басқаруды қамтамасыз етеді, файлдарды резервтік көшірмелеу және қалпына келтіруді және т.б. жүзеге асырады.

Пайдаланушы жүйеге кірген соң ол үшін пәрмендік түсініктеме

берушілердің (қабық) бірі іске қосылады. *Қабық* — бағдарламалық жүйелермен өзара әрекеттесу үшін құрылатын бағдарлама.

UNIX-тектес ОЖ-мен желіні бақылау және басқару оны шешу әкімшілік және техникалық басқарушылықты сақтауға мүмкіндік беретін міндет болып табылады.

Әкімшілік міндеттер, әдетте, желінің түрлі нысандары арасында желілік ресурстарды үлестіру және олардың әрекеттерін үйлестірумен байланысты. UNIX жүйесінде иеленуші және файлмен байланысты артықшылықтар туралы нұсқауларды сақтау әдістері негізгі мәселе болып табылады. Әдетте, пайдаланушымен іске қосылған процесс осы пайдаланушыға тиесілі қолжетімділікке деген артықшылықтарға ие. Алайда, әкімшілер пайдаланушылар қолжетімділігіне рұқсат еткілері келмейтін файлдарға қолжетімділіктің жүйелік пәрмендері бар. Әкімші барлық қауіпсіздік мәселелерін басқарып отырады. Ол жүйедегі өзгерістердің тұрақты мониторингін жүргізіп отыруы және зиянкесті араласуларға қарсы әрекет жасай алуы керек. Сақтандырушы әкімшіліктендірудің идеясы автоматтандырылған ақпараттық жүйе немесе оның жекелеген құрауыштарының әрекеттеріне талдау жүргізіп, ақыры жаман болатын оқиғаның дамуына жол бермейтін алдын алу шараларын қабылдауда болып табылады. Жүйелік әкімшілер бұзушы әрекетінің моделін нақты танып білуі керек.

Linux— UNIX-тің еркін таратылатын нұсқасы. Онда ядро құруға ерекше назар аударылған. Оны ашық бағдарламалық код ерекшелейді. ОЖ пайдаланушының нақты қажеттіліктеріне түрлендіруге болатын бастапқы мәтін түрінде жеткізіледі. Linux тегін таратылады және көпішілік пайдаланатын көп мәселелі жүйе үшін ең қарқынды дамып жатқан ОЖ боылп табылады. Бұл икемді толыққанды көп мәселелі көпшілік пайдаланатын UNIX-тектес ОЖ X Windows графикалық жүйесімен жұмыс істейді. Бұл кезде нақты көпшілік қолданатын және көп мәселелі тәртіп қамтамасыз етіледі.

X Windows (XWindow жүйесі немесе қысқаша — X) — UNIX-машиналарға арналған стандартты графикалық көптерезелі және көп терминалды интерфейс.

Заманауи маңызды бағдарламалық пакеттердің көпшілігі Linux платформасы үшін жүзеге асырылған. Бұл ерекше операциялық жүйе (ОЖ). Оны тиімді пайдалану үшін оны жобалау ерекшеліктері мен философиясын түсіну маңызды. Бұл күрделі мәселелерді шешуге және үлестірілген есептеулерді ұйымдастыруға арналған үлкен және қуатты жүйе.

Linux дамуы үшін жауап беретін нақты бір ұйым жоқ.

Linux қолдану аясын кеңейту кезінде туындаған проблемаларды айқындайтын анықталған қателер туралы ақпарат кодтарымен алмасатын

еріктілер тобымен «қоғамдық бастамаларда» (freeimplementation) жұмыс істейді және дамиды. ГТШЧ үшін Интернетте еркін таралатын бағдарламалардың көпшілігі айтарлықтай өзгеріссіз Linux үшін қайта құрастырылуы мүмкін.

Linux орнату және қолдануда өте қарапайым. Ол TCP/ IP (FTP, Telnet, NNTPи SMTP) желілік жұмыстар мен қызметтер үшін TCP/IP хаттамаларының толық жинағын қамтамасыз етеді. Linux ядросы дисктен жадыға бағдарламаның нақты қолданылатын сегменттері жүктелетін кездегі қажетті парақшалардың жүктелуін ғана қолдайды. Бір парақша бірнеше орындалатын бағдарламалармен қолданылуы мүмкін. Дисктегі қолжетімді жадының көлемін ұлғайту үшін свпинг немесе фиртуалды жадыға арналған кеңістік бөлінуі мүмкін. Жүйеге физикалық жадының үлкен көлемі қажет болған кезде ол свопингтің көмегімен белсенді емес парақшаларды дискке жазады, бұл әлдеқайда ауқымды бағдарламаларға орындауға және біруақытта пайдаланушылардың көп санына қызмет көрсетуге мүмкіндік береді. Свопинг физикалық жадының ұлғаюын жоққа шығармайды, себебі, ол тез әрекеттілікті төмендетеді және қолжетімділік уақытын ұлғайтады.

Орындалатын бағдарламалар үдемелі байланысты кітапханаларды қолданады, яғни, олар бір физикалық файлмен дискте ұсынылған кітапханалық бағдарламаны бірлесіп қолдануы мүмкін. Бұл орындалатын файлдарға, әсіресе, кітапханалық қызметтерді бірнеше рет қолданатын файлдарға дискте аз орын алуға мүмкіндік береді. Сонымен қатар, нысаналы кодтар деңгейінде ретке келтіруді қолданғысы немесе бөлінетін кітапханаларды қажет етпейтін орындалатын бағдарламалар алғысы келетіндер үшін статикалық байланысты кітапханалар да бар. Linux-те бөлінетін кітапханалар орындалу кезінде үдемелі байланысып, бағдарламашыға кітапханалық модульдерді өз модульдерімен алмастыруға мүмкіндік береді.

Linux, басқа да UNIX-жүйелерде бар барлық стандартты кітапханаларды, бағдарламалық аспаптарды, компиляторларды, ретке келтіргіштерді қоса алғанда, бағдарламалаудың толық UNIX-ортасын қамтамасыз етеді. Кәсіби UNIX-бағдарламашылар мен желілік әкімшілер Linux-ті үй компьютерлерінде қолданып, олардан жазылған бағдарламаларды ұйым (фирма) компьютерлеріне көшіре алады. Мұндай әдіс уақыт пен қаражатты үнемдеуге мүмкіндік береді, үй компьютеріндегі жайлы жұмысты қамтамасыз етеді.

Жүйе өздігінен ашық қағида бойынша жобаланады. Ядроның жаңа нұсқалары шамамен бірнеше аптада бір рет пайда болады. Жаңа бағдарламалар тұрақты пайда болып отырады. Мұндай қарқынды есепке ала отырып, көптеген пайдаланушыларға ең дұрысы жекелеген

жетілдірулер жасап отырған жөн, яғни, ОЖ-ның жаңартуды қажет ететін бөліктерін ғана ауыстырып отыру қажет.

Linux-те жүйені пайдаланушылардың жеке қажеттіліктеріне қарай күйге келтіруге болатын графикалық қбықшалардың бірнеше түрі бар. Linux-ті пайдалана отырып, UNIX-тің практикалық міндеттерді орындау үшін қажетті барлық негізгі ерекшеліктерін меңгеріп алуға болады. Білім алушылар, бағдарламалауды меңгерушілер UNIX-те бағдарламалуды үйрену және ядро архитектурасын меңгеру үшін Linux-ті пайдалануларына болады. Linux арқылы кітапханалар мен утилиталардың толық жинағына, сондай-ақ, ядроның бастапқы мәтіндері мен кітапханаларына қол жеткізуге болады.

Windows секілді ОЖ-мен желілерде әкімшіліктендіру міндеттерінің есепке алуды қажет ететін бірқатар ерекшеліктері бар.

Жүйелік құралдардың басым бөлігі оны іске қосатын пайдаланушыдан әкімшілік артықшылықтардың болуын талап етеді. Жүйені басқару бойынша операцияларды орындау мүмкіндігі болуы үшін сәйкес құқытары бар жүйеде есеп жазбасы бойынша тіркелуі керек. Алайда, қауіпсіздік ережелері жүйеде мұндай есеп жазбаларын тұрақты қолданбауды талап етеді.

RunAs командасы әкімшіге онда есеп жазбасы арқылы құқықтары шектеулі артықшылығы жоқ пайдаланушы ретінде тіркеліп, жүйені басқару бойынша барлық жұмыстарды орындауға мүмкіндік береді. Оның көмегімен әкімші қажетті құқытары бар әкімшінің есеп жазбасын немесе пайдаланушының есеп жазбасын іске қосып, «артықшылығы юар» пайдаланушының атынан кез-келген утилиталарды іске қоса алады. RunAs командасын ActiveDirectory файлдарына немесе нысандарына қолжетімділікке пайдаланушылық рұқсатнамаларды орнату немесе тексеру үшін қолдануға болады. Пайдаланушыға рұқсат беру үшін әкімшілік артықшылықтары бар сәйкес утилитаның іске қосу қажет. Біруақытта қарастырылып отырған пайдаланушының құқықтары мәнмәтінінде қажетті қосымшаны іске қосуға және қорытынды рұқсаттарды тексеруге болады.

Есеп жазбалары мен топтар құру Windows қауіпсіздігін қамтамасыз етуде ерекше орын алады. Қолжетімділік құқығы мен артықшылықтар тағайындай отырып, әкімші пайдаланушылардың желідегі құпия ақпаратқа қолжетімділіктерін шектеу, желіде белгілі бір әрекетті орындауға рұқсат ету немесе тыйым салу құқығына ие болады, мысалы, мәліметтерді мұрағаттау немесе компьютер жұмысын аяқтау. Windows жүйелерінде серверді әкімшіліктендіру бойынша қажетті операцияларды орындау үшін қашықтықтан қосылуға мүмкіндік беретін RemoteDesktopforAdministration немесе RemoteDesktop стандтартты механизмі бар. Әкімші кез-келген жұмыс орнынан серверге қашықтықтан қосылып, оны басқара алады. Қашықтықтан әкімшіліктендіру механизмін терминалдар қызметінен бөлу

серверді басқа компьютерден басқару кезінде серверге түсетін жүктемені минимумға жеткізуге мүмкіндік берді.

Сонымен қатар, пайдаланушыға өз компьютеріне қолжетімділікке бастамашылық етуге және қиын жағдайларда көмек алуға мүмкіндік беретін RemoteAssistance қызметтері де бар. RemoteAssistance қызметін қосқан кезде компьютерді қашықтықтан басқаруға да рұқсат беріледі.

Пайдаланушы профилінде жұмыс ортасының барлық баптаулары сақталады, мысалы, экран мен желіге қосылу баптаулары. Олар автоматты түрде сақталады.

Жү еге кіру сценарийі . bat немесе . cmd кеңейтілуі бар пакеттік (командалық) файлды, . exe кеңейтілуі бар атқарушы файлын немесе пайдаланушының жүйеге тіркелуі немесе одан шығуы кезінде іске қосылатын VBScript сценарийі юолып табылады. Ол желімен қосылуды орантуға немесе қосымшаны іске қосуға арналған командалардан тұруы, іздеу жолдарын көрсететін айнымалы ортаның мәндерін орнатуы, уақытша файлдарға арналған каталогтар және басқа да осы тектес ақпараттардан тұруы мүмкін. Сценарийлер сервері Windows ОЖ-да қарапайым қуатты және икемді сценарийлерді қолдануға рұқсат етеді. Бұрындары Windows ОЖ-дағы сценарийлер тілі тек қана MS- DOS командалар (командалық файл) тілі ғана болды. Бұл тез әрі шағын тіл, бірақ, VBScript пен Jscript тілдерімен салыстырғанда шектеулі мүмкіндіктерге ие. ActiveX сценарийлер архитектурасы біруақытта MS-DOS командалар жинағымен сәйкестікті сақтай отырып, VBScript пен Jscript сценарийлер тілдерін қолдануға мүмкіндік береді. Іздеуді конфигурациялау, белгілі бір бағдарламаларға жады бөлу және қосымшаларды басқару үшін Windows ОЖ жүйе мен пайдаланушының айнымалы ортасын (environmentvariables) қолданады. Бұл айнымалылар ОЖ-да орнатылатын MS-DOS-қа ұқсайды, мысалы, PATH пен TEMP.

Жүйелік айнымалы орталар компьютерде кім тіркелгеніне тәуелсіз анықталады. Бұл кезде, Administrators тобының мүшесі жаңа айнымалылар қоса алады немесе олардың мәндерін өзгерте алады.Пайдаланушының айнымалы ортасы компьютердің әрір нақты пайдаланушысы үшін жеке орнатылады. Айнымалы ортаның өзгертілген мәндері тізілімде сақталады.

Аудит — қауіпсіздікке қатысы бар оқиғаларды тіркеу процесі: жүйелегі тіркеу, файлдық жүйе нысандарын құру әрекеті, оған қолжетімділік алу немесе жою. Мұндай оқиғалар туралы ақпарат ОЖ оқиғалар журанылының файлында сақталады. Осылайша алынған ақпаратты (Security журналы) EventViewer (Оқиғаларды көру) утилитасының көмегімен көруге болады. Аудитті баптау процесінде бақылануы тиіс оқиғалар көрсетіледі. Журналдың әрбір жазбасы орындалған әреке түрі, оны орындаған пайдаланушы және аталған әрекет орындалған уақыт сәті туралы мәліметтерді сақтайды. Аудит білгілі бір

әрекетті орындаудың кез-келген талпынысын бақылауға мүмкіндік береді. Оқиғалар журналында барлық орындаулар талпынысы, соның ішінде, рұқсат етілмеген әрекеттер де көрсетіледі. Аудитті баптау үшін әкімші құқығына ие болу керек.

Тапсырмалар жоспарлаушысының (TaskScheduler) көмегімен жүйеге қызмет көрсетуге арналған командалық файлдарды, құжаттарды, қарапайым қосымшаларды немесе түрли утилиталарды іске қосудың кестесін әзірлеуге болады. Бағдарламалар жүйені жүктеу немесе оған тіркелу кезінде, сондай-ақ, жүйенің әрекетсіздігі (idlestate) кезінде бір рет, күн сайын, апта сайын немесе ай сайын белгіленген күні қосылып отыруы мүмкін. Жоспарлаушы тапсырмаларды орындау үшін тапсырманың ұзақтығын, оның аяқталу уақытын, қайталанулар санын, қуат көзі күйіне тәуелділігін және т.б. қамтитын күрделі кестені тағайындай алады. Тапсырмалар бір компьютерден екіншісіне тасымалдауға болатын . job кеңейтілуі бар файл ретінде сақталады. Әкімшілер жүйелерге қызмет көрсету үшін тапсырмалар файлдарын құрып, оларды қажетті орындарға көшіре алады. Тапсырмалар папкасына қашықтықтан кіруге болады, сонымен қатар, тапсырмаларды электронды пошта арқылы жолдауға да болады. . job файлын басқа жүйеге көшіру кезінде оны қолдануға арналған рұқсатты қалпына келтіру керек, себебі, бұ құзіреттер Windows қауіпсіздік жүйесінде сақталады. Тапсырма құру кезінде тапсырма орындалатын қауіпсіздік мәнмәтінін анықтайтын пайдаланушының аты мен құпиясөзі көрсетіледі. Бұл бір компьютерде қауіпсіздікке қатысты түрлі құқықтары бар бірнеше тапсырмаларды іске қосуға мүмкіндік береді, яғни, бірнеше пайдаланушыда біруақытта жоспарланған тапсырмалардың жеке, тәуелсіз кестелері болады.

UNIX/Linux ортасында әкімшіліктендірудің бірқатар ерекшеліктері бар. Физикалық желі дайын болған соң, әкімші өз қолымен әр машинада интерфейстерге мекенжай тағайындауы қажет. Әдетте, бұл, желідегі жұмысқа арналған компьютер консолінде жүзеге асырылады. Бір жұмыс орнынан желідегі барлық машиналарды үдемелі баптау мүмкіндігі бар. Алайда, мұндай тәсілдің айқын басымдылықтарынан бөлек кемшіліктері де бар. Олардың ең бастысы – жүйедегі әрбір машинадан жұмыс статистикасы есебі. Мекенжайларды үдемелі тағайындау кезінде машина әртүрлі уақытта әртүрлі мекенжайлар алуы мүмкін, бұл, мекенжай бойынша машинаны сәйкестендіруге мүмкіндік бермейді. Көптеген трафикті талдау жүйелері мекенжай мен компьютер арасындағы сәйкестіктің өзгермейтіндігіне негізделген. Дәл осы қағида бойынша рұқсат етілмеген қол жеткізуден көптеген қорғаныс жүйелері құрылған.

Компьютерлерге тіркелген желілік мекенжайларды тағайындауға мәжбүрлейтін тағы бір себеп желі серверлерінде көпшілік пайдалану сервистерін ұйымдастыру қажеттігі болып табылады. TCP/IP-де сервистің

орналасқан жері туралы жұмыс орындарын хабарландыру механизмі жоқ. Novell немесе Microsoft желілеріне қарағанда TCP/ IP желілерінде кең түрде хабар беру қатты таралмаған. Әрбір хост өзінің баптау файлынан (мысалы, басқа желілерге шлюз немесе домендік атаулар серверлері көрсетіледі) немесе қолданбалы бағдарламалық қамсыздандырудың баптау файлдарынан қайсыбір сервистің бар екен біледі. Мысалы, WWW сервері осы желідегі осы компьютерде орнатылғаны туралы ешбір кең түрде хабар беру хабарлама таратпайды. TCP/IP желісімен тудыратын төмен трафик мұндай тәсілдік басымдылығы болып табылады. Бұдан бөлек, кез-келген жабдық TCP/IP трафигін сүзгілеуге мүмкіндік береді, бұл, желінің сегменттеуін едәуір жеңілдетеді және одан әрі оны жеңіл құрылымдалатын етеді. Қашықтықтағы файл жүйесін монтаждау үшін жергілікті торап хаттамаларын жеткізу үшін, TCP/IP бұл ауысымды өзі жүзеге асыратындықтан, желі аралық хаттаманы пайдаланудың қажеті жоқ.

TCP/IP желісін ұйымдастыру аясында ақпаратты тиімді алмасу, ақпараттық ресурстарға қол жеткізу, электрондық поштамен алмасу және т.б. үшін электрондық байланысты қолданатын программисттер мен басқа да қызметкерлердің қашықтықтағы жұмыс орындарын ұйымдастыруға назар бөлінеді. Мұндай жұмыс орындарын TCP/IP аясында ұйымдастырудың қиындығы жоқ.

TCP/IP жергілікті желісін Интернетке қосу жергілікті провайдер арқылы жүзеге асырылады. Әдетте, бұл, жергілікті желі үшін мекенжайлар топтамасы алынған мекеме болып табылады.

Брандмауэрдың тағайындалуы және қызметі. TCP/IP желілерінде туа біткен кемшілік бар – ақпарат жиінде желі бойынша ашық тапсырылатындықтан ақпаратты рұқсат етілмеген қол жеткізуден қорғаныстың орнатылған әдістері жоқ. Бұл, зиянкестің желі арқылы берілетін пакеттерді қарап шығуға және TCP/IP-желілері пайдаланушыларының құпиясөздері мен сәйкестендіру топтамаларын алу әдістерін табуы мүмкін екенін білдіреді. Осы секілді әрекеттерді жүзеге асыру әдістері көптеген. FTP мұрағаттары мен WWW серверлеріне қол жетімділікті ұйымдастыру кезінде де осы секілді мәселелер туындайды. Сондықтан, жалпы қауіпсіздік саясаты TCP/IP-желілерін әкімшіліктендірудің негізгі қағидалары болып табылады: әкімші «қайсыбір ақпараттық ресурстарды пайдалануға кімнің, қайда және қайдан құқықтары бар» секілді ережелерді орнатады.

Желілердегі бұл мәселелер, әдетте, арнайы қорғаныс бағдарламаларын және бағдарламалық-техникалық құралдарды – брандмауэрлерді (Firewall — желіаралық сүзгілерді) – орнату жолымен шешіледі.

Қауіпсіздікті басқару бағдарлар кестесін басқарудан басталады. Бағдарларды статикалық әкімшіліктендіру соңғысын қосу және сөндіру қолмен жүзеге асырылады, ал, динамикалық әкімшіліктендіру кезінде бұл

жұмысты динамикалық бағдарландыруды қолдау бағдарламалары орындайды. Келесі кезең – домендік атаулар жүйесін басқару, домен сипаттауын көшіруге рұқсатттарды белгілеу және IP-мекенжайларын алуға тапсырысты бақылау. Келесі кедергі - TCP/ IP трафигін сүзгілеу жүйесі. Мұндай күрестің ең көп тараған құралы Firewall жүйесі болып табылады. Осы бағдарламаларды пайдалана отырып, белгілі-бір мекенжайлардан пакеттерді қабылдауға және белгілі-бір мекенжайларға пакеттерді жіберуге болатын хаттама номері мен порт номерін анықтауға болады. Ең соңғы қорғаныс құралы – трафикті шифрлеу. Бұл мақсат үшін қоғамдық желі арқылы қорғалған алмасуды ұйымдастыру үшін әзірленген түрлі бағдарламалық қамсыздандыру пайдаланылады.

Брандмауэр мен прокси-сервердің (proxyserver) қызметтерін айыра білу қажет. Прокси-сервер – жергілікті желіде Интернеттің шығу және кіру трафигін басқаратын арнайы интернет-сервер.

Прокси-сервер келесі қызметтерді атқарады:

- Мекеме желісіне хабарландырулар мен файлдарды тапсыру қауіпсіздігін анықтайды;
- Желіге қолжетімділікті басқарады;
- Берілген параметрлерге сәйкес сұраныстарды сүзгілейді және қабылдамайды.

Прокси-сервер Интернеттен мәліметтерді жинайды және жергілікті желдегі браузерлерге сұраныстар бойынша тапсырады. Бұл мәліметтер бөлінетін (жалпыға қолжетімді) кэште сақталады. Егер, бұл ақпарат қайтадан сұратылса, онда, ол кэштен алынады. Кэш жергілікті есептеуіш техникасының ішінде болатындықтан, мәліметтерді жолдау Интернеттен гөрі жылдамырақ жүзеге асырылады. Кэш негізінде Интернетке қолжетімділік жылдамдығын кірген сайттардан мәліметтерді жергілікті ұсыну арқылы ұлғайтады, осылайша, ол Интернеттен мәліметтерді тек кірмеген жерлерден алуға мүмкіндік береді. Нәтижесінде, коммуникациялық ресурстарды өзгертусіз өнімділік жақсартылады.

Қолжетімділікті басқару WWW-серверін пайдаланушыларының қолжетімділік құқығын шектеуге мүмкіндік береді. Прокси-сервер Интернет ресурстарына қолжетімділікті басқару үшін пайдаланыла алады. Мысалы, кейбір пайдаланушыларға белгілі-бір Web-сайттарға қолжетімділікті шектеу. Шектеу бөлек пайдаланушыларға, пайдаланушылар тобына немесе бөлек URL-ге қатысты болуы мүмкін. Әрбір тыйым салынған URL-де онымен байланысқан осы URL-ге қолжетімділігі бар пайдаланушылар мен топтар тізімі бар. Қолжетімділікке рұқсат алу үшін браузердің сұранысы бойынша олар аты мен паролін енгізулері қажет. Сонымен бірге, тыйым салынған URL-дер «Әкімшілер» тобының мүшелеріне әрқашан қолжетімді.

КОМПЬЮТЕРЛІК ЖЕЛІЛЕРДІҢ БАҒДАРЛАМАЛЫҚ ҚАМСЫЗДАНДЫРЫЛУЫН ПАЙДАЛАНУ

I

БӨЛІМ

1-тарау. Web-серверді орнату
2-тарау. Брандмауэр орнату және параметрлері

1 тарау

WEB-СЕРВЕРДІ ОРНАТУ

1.1. WEB-ИНДУСТРИЯСЫНЫҢ ДАМУЫ

Рунет экономикасы 2012 жылы Ресей ЖІӨ-нің 1,3%-ын құрады. Мұндай мәліметтер ресейлік интернет-индустрияның ірі ойыншыларының қолдауымен Ресей электронды коммуникциялар қауымдастығы (РЭКҚ) мен «Экономика жоғарғы мектебі» ұлттық зерттеу университеті (ЭЖМ – ҰЗИ) өткізген «Рунет экономикасы 2012-2013» зерттеуінің таныстырылымы барысында ұсынылды.

Зертеу мәліметтері бойынша контент пен сервистер нарығының көлемі 563 млрд. р., ал электронды төлемдер нарығы 268,7 млрд.р. құрады, бұл жалпы алғанда 2012 жылғы Ресейдің ЖІӨ-1,3%-ын құрайды. Бұл кезде, ішіне Интернетке қолжетімділік, электронды B2B-коммерция және интернет компанияларына инвестициялар кіретін интернетке тәуелді нарықтардың экожүйесінің көлемі 4,3 трлн. р. құрады, бұл Ресей ЖІӨ-нің 6,9%-мен салыстырмалы.

2013 жылы интернет экономиканың зерттелген сегменттерінің оратша өсімі өткен жылғы көлемінен 25%-да кем болмады, бұл Ресей Федерациясының, сондай-ақ, ел экономикасының көптеген жекелеген сегменттерінің жалпы экономикасының орташа өсімінен әлдеқайда жоғары.

Зерттеу барысында жарнама мен маркетин индустриясының едәуір белсенді және ірі нарығына баға берді. Айтарлықтай өсім мен даму интернет-сайттарын әзірлеу, Интернетте жарнама орналастыру, әлеуметтік медиа- және іздеу жүйелерінде тауарлар мен қызметтерді сүйемелдеу бойынша қызметтер саласында байқалады. Осылайша, медиялық жарнама нарығының көлемі 2014 жылдың қаңтар-қыркүйек аралығында 19,20 млрд. р. құрады, бұл 2011 жылғы көрсеткіштен 118%-ға артық. 2015 жылғы күтілетін өсім тағы 16%-ды құрайды.

Мәнмәтіндік жарнама 2012 жылы көлемі бойынша 37,55 млрд. р. құрады, бұл 55% өсімге тең. 2013 жылы нарық өсімі 34%. Интернеттегі бейнажарнама көрермендерінің аудиториясы 2014 жылдың бірінші жартыжылдығында 63 млн. адамды құрады. Бұл 2013 жылдың балама

кезеңіндегіден 11%-ға артық. 2013 жылы іздеуді оңтайландыру 10,24 млрд. жинады, бұл пайыздық көрсеткіште 20%-ға артық өсімді көрсетті. Әлеуметтік желілердегі маркетинг пен коммуникация нарығы 2013 жылы 6,3 млрд. р. бағаланды, ол 2014 жылы 17%-ға өсті.

Домендік нарық көлемі 2013 жылы 2,5 млрд. р., хостинг-индустрияның көлемі 4,38 млрд. р. құрады. Рунеттегі SaaS-шешімдер (бағдарламалық қамсыздандыру қызмет ретінде) нарығының көлемі 2013 жылы 4,3 млрд. құрады.

Ақырында, Интернет арқылы ойын қосымшаларын жеткізу, әлеуметтік желілердегі және мобильдік платформалардағы ойындарды, сондай-ақ, ойын қосымшалары ішінде виртуалды тауарлар мен сервистер сатуды қоса алғанда, ойын нарығы өзінше жеке бағаланды. Ойын нарығының көлемі 2012 жылы 28,58 млрд. р. құрады.

Интернет-нарығының ең ірі сегменті электронды сауда болып қала береді. Бұл секторды сарапшылар төрт сегмент бойынша зерттеді: онлайн-ретейл 284,96 млрд р. көлемінде; электронды төлемдер 268,7 млрд р. көлемінде, сондай-ақ, Интернеттегі сандық контент нарығы (видео, музыка, кітаптар), ол 5,07 млрд р. құрады. Онлайн-трэвел сегменті 153,20 млрд р. жетіп, 2012 жылмен салыстырғанда 40%-ға ұлғайды. Саяхаттар сегментіндегі өсім 2013 жылы 29%-ды құрады.

Жалпы, интернет-сауданың 2014 жылғы көлемі шамамен 22%-ға бағалануда. Оның үстіне, сарапшылар бұл сегмент үшін алдағы бес жылда өсім экономиканың қандай күйде болуына еш тәуелсіз қамтамасыз етілген деген пікір білдіруде. Негізінен, зерттеу материалдарында төрт ықтимал сценарий жайында айтылады.

Инновациялық сценарий солардың ішіндегі ең оптимистік сипаттағысы болып табылады, бұл 2018 жылға дейін нарық өсімі 35-40%-ды құрайды дегенді қарастырады. Оны жүзеге асыру тек іскерлік климатты ұлғайту мен жалпы жағымды экономикалық ахуал барысында ғана мүмкін. Сонымен қатар, бұл нұсқа ішкі нарықты ынталандыру бойынша бірқатар шараларды есепке алмағанда, мемлекет аталған саланы реттемелеуге араласпайтынын да қарастырады.

Тұрақтандыру сценарийі кезінде (Интернетті реттемелеу саласындағы заңнама ағымдағы түрінде сақталады) интернет-индустрияның көлемі 15-20%-ға, ал жағымсыз жағдайда (реттемелеуші ортаның нашарлауы, іскерлік климатпен ахуал дәл сол күйде) – 6-10%-ға ұлғаяды. Үлкен дағдарыс жағдайында нарықты орташа жылдық өсімі 3-6%-ды құрайды, бірақ, электронды коммерция секілді жекелеген сегменттерде ғана байқалатын болады.

DataInsight мәліметтеріне сәйкес, 2013 жылы трансшекаралық

интернет-сатып алулардың әлемдік нарығының көлемі 105 млрд. долларға жетті. Шетелдік интернет-дүкендердің қызметін 94 млн. шетелдік сатып алушылар қолданады. 2018 жылға қарай бұл көрсеткіштер 307 млрд. доллар мен 130 млн. адамға өседі деп күтілуде.

Интернет-сатып алушылары арасында АҚШ (45%), Ұлыбритания (37), құрлықтық Қытай (26), Гонконг (25), Канада (18), Австралия (16) және Германия (14%) саудагерлері үлкен танымалдылыққа ие.

Шетелде көбіне киім, аяқ киім мен киім-кешек керек-жарақтарын (12,5 млрд долл.), сұлулық пен денсаулыққа арналған тауарлар (7,6 млрд долл.), гаджеттер мен компьютерлік жабдықтар (6,0 млрд долл. дейін), зергерлік сән бұйымдары, бағалы тастар мен сағаттар (5,8 млрд долл.), сондай-ақ, тұрмыстық электроника (5,4 млрд долл.) сатып алады. Әдетте, адамдар «үнемдеу» (80%) және «жергілікті нарықта қол жетпейтін дүниені сатып алу» (79%) үшін шетелдік сатып алушылардан интернет-сатып алуларын жүргізеді.

1.2. WEB-СЕРВЕР ТҮСІНІГІ

Web-сервер — клиенттерден HTTP-сұраныстарын қабылдайтын, әдетте, Web –браузерлерден, және оларға HTML-парақпен, суретмен, файлмен, медиаағынмен немесе басқа да мәліметтермен HTTP-жауаптар беретін сервер.

Web-сервер деп Web-сервер қызметтерін атқаратын бағдарламалық қамсыздандыруды, я болмаса, осы бағдарламалық қамсыздандыру жұмыс атқаратын компьютерді атайды.

Web-браузер болып табылатын клиент Web-сервер бойынша URL-мекенжайлармен белгіленген ресурстарды алуға тапсырыс береді. Ресурстар – клиентке қажетті HTML-парақтар, суреттер, файлдар, медиаағындар және басқа да мәліметтер. Жауап ретінде Web-сервер клиентке сұратылған мәліметтерді береді. Бұл алмасу HTTP хаттамасы бойынша жүзеге асырылады.

Web-браузер (Webbrowse), немесе жай ғана браузер — Web-сайттарды қарауға арналған бағдарламалық қамсыздандыру, яғни, Web-парақшаларды сұрау (көбіне Желіден), оларды өңдеу, бір парақшадан келесі парақшаға өту үшін. Көптеген заманауи браузерлер FTP-серверлерден де файлдарды жүктей алады.

Браузерлер Ғаламтордың пайда болу сәтінен бастап тұрақты дамып отырды және оның дамуымен едәуір сұранысқа ие бола бастады. Бүгінгі

таңда браузер – Web-парақшаның түрлі құраушыларын өңдеуге және шығаруға арналған және Web-сайт пен сайтқа кіруші арасындағы интерфейсті ұсынуға арналған кешендік шешім. Көптеген танымал браузерлер тегін немесе басқа қосымшалармен жинақта таратылады: InternetExplorer (Microsoft Windows-пен бірге), Mozilla Firefox (тегін, еркін бағдарламалық қамсыздандыру, Linux-тың көптеген дистрибутивтерімен бірге, мысалы, Ubuntu), Safari (MacOSX-пен бірге және Microsoft Windows үшін тегін), Google Chrome (тегін), Opera (8.5-нұсқасынан бастап тегін).

Бұл тарауда Web-сервер жұмысы жөнінде айтылады. Заманауи ақпараттық технологиялар нарығы түрлі өндірушілердің, түрлі масшабталулығымен және ресурстарға түрлі талаптармен Web-серверлердің көптеген таңдау нұсқаларын ұсынады. Зерттеу компаниясының мәліметтері бойынша әлемдегі Web-серверлердің көбісі (68 %) ApacheHTTPServer-де жұмыс атқарады. Бұл, сервердің жоғары масштабталулығы және портталулығымен байланысты. Осы Web-сервердің бастапқы кодтары ApacheLicense2.0 лицензиясымен лицензияланған, демек, бастапқы кодтар ашық және кез-келген пайдаланушы оған қажетті модульдері түзете немесе жазып бітіре алады.

Танымалдылық бойынша үлкен жүктемелерге бағытталған Nginx Web-сервері екінші (17,9%) орынды алады. Бұл серверді қолданудың ең танымал әдісі оны едәуір ауыр салмақтағы Web-сервером ApacheHTTPServer алдында кэштеу тәртібінде оны орнату. Бұл, осы Web-сервердің артында ApacheHTTPServer-ді пайдалану жасырын тұрғанын білдіреді.

Кейбір белгілі Web-серверлер тізімі:

- *Microsoft* компаниясы ұсынған IIS, Windows жанұясының серверлік БҚ-да таратылады;
- Lighttpd — еркін Web-сервер;
- GoogleWebServer—Apache-де негізделген және *Google* компаниясымен толықтап жазылған Web-сервер*;*
- Resin—қосымшаның еркін Web-сервері;
- Cherokee— тек Web-интерфейс арқылы басқарылатын еркін Web-сервер;
- Rootage— Java-да жазылған Web-сервер;
- THTTPD— қарапайым, шағын, жылдам және қауіпсіз Web- сервер.

1.3 ЖЕҢІЛСАЛМАҚТЫ WEB-СЕРВЕРЛЕР

Жеткілікті түрдегі жеңілсалмақты (жеңіл деп аталатын) серверлер нарық көшбасшылары мен басқа «ауырсалмақтыларға» қолжетімді емес мүмкіндіктерге қол жеткізе алады. мысалы, бүкіл сервер бір файлға сыйғызыла алады.бұл, әзірлеуші үшін өте ыңғайлы. Себебі, тиімді жұмыс атқару үшін оған қажетті барлық құралдарды өзімен бірге таси алады; егер, Сіз өзіңіздің Apache өндірістік серверін қолданған болсаңыз да, орнатуы бірнеше секундты алатын жеңіл серверді орнатып, кез-келген жерлерде отырып жаңа идеяларды сынап көре аласыз. Өзінің талап етпеушілігімен жеңіл серверлер IIS-тің «ауырлығын» көтере алмайтын машиналарда да тиімді жұмыс атқарады.

Сонымен қатар, шағын жеңіл Web-серверлер өнімділігі шағын машиналарда да тиімді жұмыс атқарады. Мысалы, өндірістік компьютерлерде қашықтықтағы жүйелерде, қиын жағдайларда немесе жеткіліксіз электр қуат беру жағдайларында қызмет атқаратын мамандандырылған жабдықтарда пайдалану қажеттігі туындайды. Бұл жағдайларда Web-парақшаларды дискте үлкен орынды немесе үлкен өнімділікті талап етпейтін қандай да бір қосымшалармен өңдеу мүмкіндігі үлкен артықшылық болып табылады; бұл дегеніміз ЭЕМ-дерде Web арқылы қолжетімді орнатылған, Apache-ге тән үстеме шығындарсыз және әзірлемесі күрделі емес басқарушы консольдер тән дегенді білдіреді.

Барлық дерлік жеңіл Web-серверлердің қандай да бір дәрежеде бастапқы коды бар болады. Егер, Web-сервердің ерекше әрекеті қажет болса, онда келесі сипатталған серверлердің кішкентай болғаны соншалық, оларды түсіну оңай және сәйкесінше, жетілдіру де оңай (бірнеше ерекшеліктер ғана бар). Бұл Web-серверлер Web-серверлер арнайы жабдыққа немесе жалпы пайдаланудағы компьютерлердегі жұмыстарға арналған ерекше қосымшаларға орнатылатын жобалар үшін керемет бастапқы материал болады. Олар сол сияқты қарапайым Web-сайттарда кеңінен қолданылады.

- YouTube мұрағатталған контентті, мысалы бейнені жедел жеткізу үшін lighttpd қолданады;
- cdServe болса «German Woodworking Machinery and Tools» CD-дисктерінде жұмыс істейді;
- LiteSpeed болса twitter, www.funnyoride.com, www. airliners. com, WordPress.com, fanfiction.com, SlashGear, www.forumac- tif. com және басқа да белгілі Web-сайттарды «анықталды»;
- OpenSUSE, RubyOnRails, MarkaBoo және бірқатар басқа белгілі сайттар Mongrel-ге сүйенеді;

- THTTPD болса ht. com, mtv. com, The Drudge Report, garfield. com және басқаларда жұмыс істейді.

Жеңіл серверлер жоғарыда аталған ауқымды бірқатар сайттарды қоса алғанда, тіпті нақты есептеуіш орталықтарда да өз рөлдерін ойнайды. Ерекше жоғары өнімділікті сайттар кэштеу, прокси-серверлер және т.б. максималды пайда алу үшін өз операцияларын сегменттейді. Apache негізіндегі сайтта, мысалы, баяу өзгеретін кескіндер белгіленген файлдық жүйеден «минималистік» Web-сервер арқылы жеткізілетін архитектурасы болады. Ақырғы пайдаланушы нақты нені көретіні – бұл Apache-дің және әрқайсысы басқалардан асып түсетін рөлді ойнайтын бірнеше қосымша Web-серверлердің командалық жұмысының нәтижесі. Мұндай конструкция есептеуге жұмсалатын өте аз шығынмен өте жылдам нәтижелер беруі мүмкін.

Жеңіл Web-серверлердің ортақ қасиеттері көп болғанымен, аталған дәреженің ішінде айырмашылықтар да бар. Серверлердің басым көпшілігі C тілінде жазылған, бірақ, серверлердің ішінде басқа тілде жазылған бірқатар сәтті жүзеге асырулар да бар, олардың қатарында Erlang, Java, Lisp, Lua, Perl, Pythonи Tcl. Егер, сіз қандай да бір тілді қалайтын болсаңыз, онда сол тілде жазылған Web-сервер табуыңыз әбден мүмкін.

«Сирек» тілді таңдау себептері айрықша болуы мүмкін.

1. *Білім.* Жеңіл Web-сервермен жұмыс — байыпты, бірақ, шамадан тыс жұмыс емес. Бұл тілмен жұмыс істеу тәжірибесін алудың жақсы әдісі.
2. *Кооперация.* C тілінде жазылған жеңіл Web-сервер әдетте 10-15 Кбайт болса, ал жоғары дәрежелі тілдердің атқарылатын файлдары 100 Кбайттан бірнеше мегабитқа жететін болса, жоғары дәрежелі тілдегі толық Web-серверге арналған бастапқы код бар болғаны бірнеше мыңдаған байтты ғана құрауы мүмкін. Apache-ні түрлендіргенше мұндай бастапқы кодты әріптестермен бірге қолдану айтарлықтай жеңіл.
3. *Зерттеу.* Жоғары дәрежелі тілдер эксперименттерді айтарлықтай жеңілдетеі, мысалы, жаңа мүмкіндіктерді қосу үшін HTTP/1.1 небәрі бірнеше қосымша код жолдарын талап етуі мүмкін. Бұл жеңіл серверлер – қолайлы эксперименталь материал.
4. *Түрлендіру.* Жоғары дәрежелі тілде жазылып қойған, қазіргі уақытта бар қосымшаға HTTP-сервер қосу бастапқы кодты недбәрі бірнеше жолға ұлғайтуды талап теуі мүмкін.

Бұл жерде Athana жақсы мысал бола алады. Бұл Web-сервер, Python-да жзылған. Ол HTTPmultipart (uploading), сессияларды, Cookies және басқа да көптегендерді қолдайды. Athana, қазіргі уақытта 0.2.1 нұсқасында әрекет етуші ол мінсіз құрастырылған бастапқы файлға сыяды.

Бұған дейін айтылғандай, жеңіл Web-серверлердің мүмкіндіктері қолданылған тілге белгілі бір деңгейде тәуелсіз өзгеріп отырады. Барлық жеңіл Web-серверлер Apache-ге қарағанда шағын және жеңіл конфигурацияланады. Олардың кейбірі Apache-ден жылдам, кейбірі өте жылдам; кейбіреулерінде қауіпсіздікке, үлкен жүктеме кезіндегі үздіксіз жұмысқа, жады кеңейтілуі немесе үнемделуіне баса назар аударылған. Қалай болғанда да олармен танысып шығуға болады, ал бұл істе Apache кейіндеп тұр.

Бұл мүмкіндіктердің артында қандай нақты өнімдер тұр? Деңіл серверлермен шектеліп отырсақ та біз нанғысыз үлкен таңдауға тап боламыз. Серверлерді шағын топтарға жіктейді: ультражеңіл, аса қорғалған, ерекше тілді қолданушы және т.б.

Осы топтардың ішінен ультражеңіл Web-серверлер ерекшеленеді, бұл Apache-ден әлдеқайда кіші серверлер. Мұндай көлемдегі қосымшалардың қауіпсіздігі мен масштабталулығын дәлелдеу үшін олардың жұмыстарын жйелі және қатаң түрде елестету керек. Өте шағын Web-серверлерге мыналар жатады:

- *CheetahServer* — C тіліндегі жолдары 1 000-нан аз;
- *DustMote* — көлемі шамамен 3 000 байт болатын TCL-негізгіде жүзеге асырылған өте шағын Web-сервер;
- *Fnord* — платформасы және конфигурациясына байланысты 20 Мбайттан кем орынды алады. Көлемінің шағын болуына қарамастан ол фиртуалды хостингті, CGI және keep-alive қолдайды;
- *Ihttpd* — 800-ден аз C жолы бола тұра, CGI қос алғанда, inetd арқылы парақшаларға қызмет көрсете алады;
- *Mattows* — CGI қолдайды, бұл жағдайда C-дегі небәрі 600 жолды құрайды;
- *Scrinchy* — шағын – шамамен 30 Мбайт көлеміне қарамастан, Sy деп талатын мамандандырылған стектік тілді қоса алғанда көптеген сценарийлер тілдерін қолдайды;
- *ZWS* — мазмұнды қосымшаны қалай жазуға болатынын көрсетеді — бұл жағдайда HTTP0.9+ сервер — көп дегенде 500 жолмен жақсы түсіндірілген zsh(!). Көлемінің шағын болуы бұл серверлерді байыпты қодданауға кедергі келтірмейді: fnord, мысалы, мыңдаған біруақыттағы қосылуларға қызмет көрсетеді.

Жеңіл серверлердің жетістіктері бойынша таң қалдырарлық топтарының бірі – бұл өнімділігі жоғары серверлер:

- *Cghttpd* — шағын Web-сервер, оны Linuxсерии 2.6 ядроларында қолжетімді асинхронды құралдарды қолдану бойынша эксперимент ретінде қарастыруға болады;

- *Darkhttpd* — жылдам бірағынды HTTP/1.1 сервер;
- *Gatling* — жоғары өнімділік үшін арнайы әзірленген. FTP, IPv6, виртуалды хостинг, CGI және т.б. қолдайды;
- *Kernux* — HTTP-демонының орындалуын қамтамасыз ететін Linux ядросының модулі;
- *Lighttpd* — әлемдегі танымалдылығы бойынша бесінші Web-севрер (және оның үлесі әлі де өсуде!). Ол біруақыттағы қосылулардың көп санына оңтайландырылған: «Әдеттегі сценарий — статикалық контентті беруге арналған негізгі серверді босатушы ретінде lighttpd қолдану...»;
- *LiteSpeedWebServer* — коммерциялық жеңіл Web-сервер, мұнды өнімділік пен қауіпсіздікке баса назар аударылған. *LiteSpeedTechnologiesInc.* статикалық контент үшін алты есе және түсініктеме беруші парақшалар үшін бірнеше қарапайым көрсеткіштер жайында мәлімдейді;
- *MiniatureJWS* — tjws ретінде танымал Web-сервер. Java-ға жазылған, сервлеттерді, JSP және мыңдаған параллель қосылуларды өңдеп, небәрі 77 Кбайт орын алады. Оның авторы бұл серверді былай сипаттайды: «Apache2.x.-ке қарағанда 10%-ға жылдамырақ»;
- *Yaws* —Erlang-ке жазылған өнімділігі жоғары HTTP/1.1 сервер.

Көптеген Web-серверлер үлкен қосымшаларға кіріктіру үшін әзірленген топтар немесе кітапханалар түрінде іске асырылған. Олардың ішінде, әсіресе, мыналар қызықты:

- *EHS* — кіріктірілетін HTTP-сервер, C + + тобы, C++ қосымшаларға кіріктіру үшін әзірленген;
- *EmbeddedTCLWebServer* — қарапайым Web-сервер, SSL және BasicAuthentication қолдайды және бұл жағдайда адам сенгісіз өте жылдам — автордың өлшеулері бойынша lighttpd және AOLserver-ден кем түспейді. TCL жүзден аз жолдары бар.

Python тілінде бірнеше Web-серверлер жүзеге асырылған, олар ерекше биіктіктерден көрінеді:

- *cdServer* — Python-дағы шағын қарапайым HTTP-сервер, CD-ROM-нан контент (статикалық) беру үшін әзірленген. Үдерісті контентке қызмет көрсетуде шектеулі мүмкіндіктерге ие. «Бұзылмайтын liveCD» жеткізуін құрайтын бірнеше жобалар бар және cdServer түріндегі құралдар олар үшін қиындау болады;
- *edna* — HTTP-да негізделген Python-дағы өте ақылды MP3-сервер.

Perl және басқа да аса қатты танымал емес тілдерде жүзеге асырылған өзге де қызықты жеңіл Web-серверлер бар:

- *Camlserv* — толық Web-сервер, ол ocaml-де жазылған және

интерактивтілігі жоғары Web-парақшаларға бейімделген. Бірнеше мыңдаған ocaml жолдарына сыйып кетеді, олардың басым бөлігі MySQL және HTML жұмыстарының ерекше мүмкіндіктеріне арналған;

- *Dhttpd* — барлық өтініштерді Apache-дікіндей форматта хаттамалайды. CGI, виртуалды хостинг, IPv6, өткізгіштік қабілетін басқару және қауіпсіздік мүмкіндіктерін қолдауға арналған кіріктірілген Perl-интерпретаторы бар;
- *DNHTTPD* — UNIX® үшін Perl-де жазылған. Ол виртуалды хосттарды, SSL-қосылуларды, CGI және т.б. қолдайды;
- *Jellybean* — HTTP-де негізделген Perl-де жазылған PerlObjectServer сервер;
- *lns. http* — LISPHTTP/1.1-дағы жалпы Web-орта;
- *Mongrel* —Ruby-де жазылған HTTP-ке арналған сервер мен кітапхана;
- *Nanoweb* — PHP-те жазылған жедел, төзімді Web-сервер. HTTP/1.1 сәйкестігін, сұраныстар бақылауды, аутентификацияны, виртуалды хостингті, SSL-сәйкестікті және т.б. қоса алғанда мүмкіндіктердің кең тізімі бар;
- *Naridesh* — Perl-де жазылған Web-сервер;
- *OpenAngel* — Perl-де жазылған. Оның фокусы – қауіпсіздік;
- *Xavante* — Lua-да жазылған HTTP/1.1 Web-сервер;
- *XSP* — C#-де жазылған және ASP. NET жетекші торабының рөлін атқарады;

Бір кезде C тілінде жазылған қосымша ерекше мүмкіндіктері бар басқа да жеңіл Web-серверлер қажет болады:

- *ABYSS* — UNIX пен Win32 арасындағы тасымалданатын сервер және Web-сервермен толық HTTP/1.1-сәйкес болуға талпынады. Жадыны пайдалануда үнемді;
- *Anti-WebHTTPD* (сондай-ақ Anti-Web, awhttpd және AW) — бір процесті (көп ағынды емес), қауіпсіздік пен қарапайымдылыққа ерекше көңіл бөлінген CGI серверді қолдайды;
- *MHTTPD* — сыртқы файлдан да, LDAP-сервердің көмегімен де MHTTPDBasicAuthentication қолдайды;
- *mini-httpd* — бір ағында параллель сұраныстарды өңдейді және жады мен процессор мәселесінде хостқа талап қоймайды;
- *NakenWeb* — көптеген басқа жеңіл серверлерге ұқсайды — BasicAuthentication, статикалық контент және т.б. қолайды. Бірақ авторлары оны Web-камералардың операцияларына арнап бейімдеген және Gumstix, WRT54GL, OpenWrt пен басқа да инновациялы платформаларда қолданған;
- *Nullhttpd* — көпағынды, бірақ, қарапайым әрі портативті Web- сервер;

- *Seminole* — коммерциялық Web-сервер,көп жадыны қажет етпейді және көп мүмкіндіктерге ие;
- Thttpd — өткізгіштік қабілетті қолдайды, chroot, BasicAuthentication және т.б. қолдайды;

Бұдан әрі қарай Web-серверді пайдалану міндеттері қарастырылады, мүмкіндігінше, жалпы ақпарат келтіріледі, алайда, барлық мысалдар мен нақты шешімдер «кеңінен тұтыну» қажеттіліктеріне әлдеқайда сәйкес сервер ретінде ApacheHTTPServer2.4 үшін ұсынылатын болады.

Көптеген алуан түрлі шағын сайттар LAMP архитектурасы бойынша құрылады. Бұл акроним мына секілді сайттардың жұмысы үшін қолданылатын бағдарламалық қамсыздандырудың атаулары ретінде түсіндіріледі: Linux— Apache— Mysql/MariaDB— PHP/Python/Perl. Linux-ті пайдалану себептері Apache себептері секілді туындап отыр:

- Ашық бастапқы код;
- масштабталушылық;
- баптау мүмкіндігі;
- тегін.

Бұл тарауда Linux ОЖ-да ApacheHTTPServer-ді пайдалану қарастырылады, нақтырақ айтсақ, openSuSELinux үлгісінде. Алайда, балама түрде сервер басқа да ОЖ-да күйге келтірілуі мүмкін: Solaris, HP-UX, *BSD және т.б.

1.4. WEB-СЕРВЕРДІ ОРНАТУ

Көптеген ОЖ үшін ApacheHTTPServer біршама алдын ала конфигурациясы бар бинарлық түрде жеткізіледі. Мысалы, оны SuSE-де жеткізу үшін

```
zypperinstallapache2
```

орындау жеткілікті.

Windows ОЖ үшін Apache дистрибутивтің бинарлық файлы форматында жеткізіледі, оны іске қосу арқылы бастапқы орнатуларды таңдай отырып, Apache-ні қосымша бааптауларсыз-ақ орнатуға болады.

Жалпы жағдайда сервердің бағдарламалық қамсыздандырылуын өз бетінше таңдауға болады. Ол үшін өндіруші сайтынан дистрибутивті жүктеу қажет (http://httpd.apache.org/). Орнату үшін келесі командаларды орындау керек:

```
tar -xvfhttpd-2.4.7.tar.bz2
```

```
cd httpd-2.4.7
./configure
make
sudo make install
```

Бастапқы орнатулар бойынша сервердің бағдарламалық қамсыздандырылуы */usr/local/* директориясына орнатылады. Егер, қандай да бір директорияларды (бинарлық, конфигурациялық файлдардың) өзгерту немесе қандай да бір модульдердің компиляциясын қосу/сөндіру керек болған кезде *configure* бойынша анықтамаға жүгіну керек:

```
./configure --help
```

Мысалы, конфигурация файлдары / *usr/local/etc*-де болмай, */etc*-те болуы керек, және пішіндері арқылы аутентификация модульдері қосымша компиляцияланууы және BASIC аутентификациясының модулі компиляцияланбауы керек. Мұндай конфигурация келесідей үлгіде болады:

```
./configure --disable-auth-basic--enable-auth-form --sysconfdir=/etc
```

Компиляция кезінде модульдер қосу және сөндіру мүмкіндігі тек қажетті қызметтері ғана бар минималды Web-серверді құрастыруды қамтамасыз етеді. Бұл сыртқы жадыдағы орынды да, жедел жадыны да үнемдеуге мүмкіндік береді.

Компиляция кезінде жетіспейтін тәуелділіктердің түрлі қателері туындауы мүмкін. Басымдылықта олар конфигурациялау сатысында анықталады:

```
configure: loadingsitescript /usr/share/site/x86 64- unknown-linux-gnu
checking for chosen layout... Apache checking for working mkdir -p... yes
checking for grep that handles long lines and -e... /usr/ bin/grep
checking for egrep... /usr/bin/grep -E
checking build system type... x86 64-unknown-linux-gnu checking host system type...
x86 64-unknown-linux-gnu checking target system type... x86 64-unknown-linux-gnu
configure:
configure: Configuring Apache Portable Runtime library... configure:
checking for APR... no
configure: error: APR not found. Pleasereadthedocumentation.
```

Бұл қателік листингі сәйкес пакет кітапханаларын жеткізу қажеттілігі туралы айтып тұр (APR). SuSE-де *zipper* командасының көмегімен пакеттердің сәйкес атауларын іздей ыңғайлы:

zypperpa| grep -iapr

Жетіспейтін пакетті мына команданың көмегімен орнатуға болады:

```
sudo zypper -n install libapr1-devel libapr-util1-devel
```

Басқа дистрибутивтерде пакеттерде басқарудың өзге де жүйелері қолданылады. Олардың өте көп болуына байланысты ол нұсқалардың барлығын қарастырмаймыз. Егер, пакеттерді басқару жүйесінің көмегімен пакетті орнату мүмкіндігі жоқ болса, ApacheHTTPServer компиляциясы жүргізілетіні сияқты бастапқы кодтардан пакет компиляциялауға болады.

Configure сәтті аяқталған соң, make makeinstall орындау қажет

Меңгеру қарапайымдылығы үшін сервердің бағдарламалық қамсыздандырылуын өз үй директорияңызға орнату қажет:

```
./configure --prefix=/home/user/httpd
```

Бұл жағдайда суперпайдаланушының есеп жазбасын қолдану қажеттілігі туындамайды.

1.5. АППАРАТТЫҚ БАЗАНЫ ТАҢДАУ

Web-серверді ұйымдастыру кезінде көптеген ерекшеліктерді есепке алу керек. Түрлі масштабталу әр алуан ресурстарды қажететеді. Web-сервердің бағдарламалық қамсызданыруы өздігінен аппараттық ресурстардың болуын талап етпейді.

Әлемде небәрі жедел сақтау құрылғысының (ЖСҚ) 20-30 Мбайт қана сәтті жұмыс істеуін қамтамасыз ете алатын жеңіл Web-серверлер де бар.

Ресуерстардың негізгі шығындары серверге жүктелген міндеттерді орындау есебінен болатынын есте сақтау керек.

TCP-порттың тыңдалуын қамтамасыз ету, бірнеше клиенттермен қосылуды ұстап тұру, виртуалдық хостингті қамтамасыз ету, қарапайым HTML-парақшаларға (алдын ала дайындалған) сұраныстарды өңдеу және бизнес-логиканың орындалуын қамтамасыз ететін басқа да бағдарламалық қамсыздандырудың шақырылуы Web-сервердің өзінің бағдарламалық қамсыздандыруының міндеті болып табылады.

Бұған дейін аталғандарды басшылыққа ала отырып, Web-сервердің өзі үшін қажетті ресурстарды болжау кезінде статикалық Web-ресурстардың беру қызметін ғана есепке алу керек. Бұл процеске келесі ресурстар қатысады:

- сыртқы жады. Бұрындары біз оларды қатты магниттік дискілер деп атайтынбыз, бірақ, ЭЕМ-дерде уақыт өте келе қатты денелі жинақтағыштар үлесі артып келеді. Сыртқы жадының жылдамдығы Web-сервердің мәліметтер жолдау өнімділігіне тікелей ықпал етеді. Егер, Web-сервер одан көлемі статикалық үлкен мәліметтерді (немесе, шағын, бірақ, бірнеше рет қайталанған) жүктеуге арналмаған болса, онда жедел сыртқы жадыға деген қажеттілік те туындамайды. Дамыған Web-сервердің келтірілген мысалы нәтижесінде 28 Мбайт дисктік кеңістікті талап етті. Тағы 50 Мбайт орнату процесі (бастапқы кодтар мен компиляцияларды ашу) үшін қажет болды;
- ЖСҚ. Дәл сол бір статикалық ресурске бірнеше рет қайталанған сұраныстар жолдау кезінде Web-сервер (мүмкін, ОЖ де) серверден жүктелетін ресурстарды кэштейтін болады. Кэштеу міндетті болып табылмайтынына және әдетте, іске қосылмаған жадыны ғана қолданып, қалдық қағидасы бойынша орындалуына қарамастан, ол жоғары жылдамдықпен сұралатын статикалық ақпаратқа қолжетімділік жылдамдығын айтарлықтай ұлғайта алады. Web-сервердің келесі келтірілген мысалы ЖСҚ-ның 104 Мбайтын тұтынады;
- орталық процессор;
- желінің өткізгіштік қабілеті.

Web-қосымшаларға қойылатын талаптар. Ашылатын Web-сервер арқылы қолжетімді Web-қосымшалардың аппараттық қамсыздандыруға қойылатын өзіндік талаптары бар. Аппараттық ресурстардың көзқарасы бойынша Web-қосымшаларды екі түрге бөлуге болады:

1) *Web-сервер процесінің ішінде жұмыс істейтін қосымшалар.* Ең кеңінен таралған нұсқа PHP қосымшалары болып табылады. Бұл жағдайда Web-қосымша Web-сервердің аппараттық ресурстарын пайдаланады;
2) *Web-серверден тыс жұмыс істейтін қосымшалар.* Мұндай қосымшалар басқа аппараттық платформада орналаса алады. Мысалы, ApacheTomcat сервері ApacheHTTPD Web-серверінің «артында» жұмыс істей алады. Бұл жағдайда Web-серверге прокси-сервер рөлінде болып, небәрі сұраныстар мен жауаптарды жолдап тұру ғана қажет. Web-қосымша жұмысының мұндай ұйымдастырылуы кезінде ол Web-сервер тікелей аппараттық ресурстарды талап етпейді және басқа аппараттық платформаға шығарылуы мүмкін.

Аутентификация жүйесіне қойылатын талаптар. Түрлі кәсіпорындарда сәйкестендіру мен аутентификациялауды ұйымдастыру үшін өз шешімдері қолданылады. Әдетте, қолжетімділікті бақылау оны

орындау үшін Web-серверге немесе Web-қосымшаға беріледі.

Қызметкерлер санының көбеюімен компания сәйкестендіру және аутентификацияның барынша күрделі құралдарына жүгінуде. Сонымен, бес адамға дейін жұмыс істейтін қызметкерлер саны бар кішігірім кәсіпорын үшін әрбір серверде немесе жұмыс станциясында пайдаланушыларды тәуелсіз баптауға рұқсат етіледі.

Серверлер мен олардың пайдаланушылары санының артуына қарай, бірыңғай пайдаланушы базасын ұстау бойынша жұмыс жүктемесі едәуір артты, пайдаланушылардың ортақ базасын құру мәселесі туындайды. NIS және LDAP сияқты сәйкестендіру мен аутентификацияның кең таралған құралдары бұл проблеманы шешімі болып табылады, растау және түпнұсқаландыру құралдарын кеңінен таратуға болады, оған түрлі серверлер пайдаланушыны түпнұсқалығын растау немесе пайдаланушы туралы қосымша ақпарат алу үшін жүгіне алады.

Ірі мекемелерде есептік ресурстарға инсайдерлік шабуылдар ықтималдығы елеулі түрде артып барады, парольді алдымен қосымша серверіне эжолдау арқылы пайдаланушының шынайылығын тексереді, содан кейін аутентификация сервері трафикті тыңдау және парольдерді ұстау мүмкіндіктері бойынша көптеген сынға ұшырайды. Мұндай жағдайларда x509 немесе Kerberos сертификаттар секілді аутентификацияның қорғалған әдістері қолданылады.

Жоғарыда аталған барлық идентификация және аутентификация нұсқалары ApacheHTTPD серверімен қолдауда болады. Орталықтандырылған идентификация және аутентификация жүйесін пайдалану осы қызметтің жүктемесін тиісті серверлерге ауыстырады және Web-сервердің аппараттық құралдарына қосымша талаптарды тудырмайды.

1.6. WEB-СЕРВЕРДІ КОНФИГУРАЦИЯЛАУ

TCP-порттарының ерекшеліктері. Заманауи компьютерлік желілерде TCP/IP желілік хаттамалар стегінен көліктік деңгейде TCP және UDP жиі қолданылады. Осы хаттамалар бойынша қосылуды орнату кезінде екі соңғы нүктелер (хосттар) порттардың нөмірлеріне сәйкес идентификацияланады. Өзгеше мақсаттар үшін қолданылатын порттардың нөмірлері IANA (InternetAssignedNumbersAuthority) бөледі және тіркейді, алайда, тәжірибеде оларды бейресми пайдалану оқиғалары жиі кездеседі.

Порттар саны 16-биттық адрестеу есебімен шектеледі (216 = 65 536, басы — «0»). Барлық порттар үш диапазонға бөлінген: жалпыға мәлім (немесе жүйелі, 0—1023), тіркелген (немесе пайдаланушылық, 1024—

49151) және үдемелі (немесе дербес, 49152 — 65535).

Бастапқыда порттардың нөмірлері NCP хаттамасымен ARPANET-те қолданылды. Жолдау жартылай дуплексті тәртіпте жүргізілді және қосу үшін екі порт қажет болды. TCP және UDP хаттамаларының қабылдануымен бір ғана порт қажетті болды және жұпты нөмірлер қолданылған жоқ — жалпыға мәлім диапазоннан кейбір порттардың тіркеуінің жоқтығы осымен түсіндіріледі.

TCP және UDP порттарының нөмірлері, сондай-ақ, SCTP және DCCP хаттамаларын қолданады. SCTP және DCCP-дегі қызметтер әдетте олардың TCP және UDP-дағы іске асыруларына сәйкес келетін нөмірлерді қолданады (бар болса).

HTTP-серверлерді пайдалану үшін IANA- порттар ресми бекітілген:

- 80 — HTTP (HyperTextTransferProtocol) — қолдану қарапайымдылығы мен трафикті оңтайландыру мүмкінедігі үшін Web-серверлердің әлдеқайда кең таралған қолданылуы;
- 443 — HTTPS (HyperText Transfer Protocol Secure) — SSL немесе TLS шифрлеуі бар HTTP.

Соңғы уақытта пайдаланушы деректерін қорғау үшін шифрлауды қолданатын интернет-сайттар саны артып келеді.

0-1 023 порты жүйелі деп саналады және пайдаланушылардың осы порттарды ашуға және тыңдауға құқықтары жоқ, сондықтан тестілік серверді іске қосқан кезде, әдетте, басқа порттарды қолданады, мысалы, 1080, 1081, 8080, 8081. 80 және 443 артықшылықты порттарында жұмысты қамтамасыз ету үшін

Следует отметить, что диапазон портов 0—1 023 считается системным и пользователи не имеют права на открытие и прослушивание этих портов, поэтому при запуске тестового сервера, как правило, используют другие порты, например 1080, 1081, 8080, 8081. Для обеспечения работы на привилегированных портах 80 и 443 Apache-де суперпайдаланушылардың құқықтары бар портты ашатын, содан кейін оны веб-сервер іске қосылатын артықшылықсыз пайдаланушыға беретін арнайы кіріктірілген механизм бар.

Web-сервер файлдары. ApacheHTTPServer, бағдарламалық қамсыздандырудың басым көпшілігі секілді мыналардан тұрады:

- сервердің жұмысын қамтамасыз ететін атқарушы файлдардан (*bin* директориясы*);*
- сервердің қосылатын модульдерінен (*modules* директориясы*);*
- конфигурациялаушы файлдардан (conf директориясы);
- HTML форматында серверді баптау бойынша құжаттамадан (*manual* директориясы*)* және man форматында атқарушы файлдардың

параметрлері бойынша құжаттамадан (*man* директориясы*);*

- Web-сервер журналдарының файлдарынан (*logs* директориясы*);*
- C/C++ тіліндегі қосымша модульдер әзірлеуге арналған файлдардың тақырыптарынан (*include* директориясы*);*
- шаблондық сайтты толтыруға арналған мәліметтер файлдарынан (*cgi-bin, htdocs*и *error* директориялары*).*

Файлдардың бұлайша орналасуы ApacheHTTPServer-дің осы нұсқасында қолмен құрастыруға арналған және әртүрлі дистрибутивтер пакеттерінің құрастырылымдарында қатты ерекшеленуі мүмкін.

ApacheHTTPServer конфигурациялық файлдары әдетте */etc/apache2* немесе */usr/local/etc/apache2* директорияларында болады. Бұл файлдарда мәтіндік түрде Web-сервердің барлық баптаулары сақтаулы болады. Конфигурациялық файлдардың мәтіндік форматы UNIX-тектес ОЖ үшін дәстүрлі болып табылады. Баптаулардың мұндай сақтаулары келесі артықшылықтарға ие:

1. Сервердің бүкіл конфигурациясы жұмыс істеп тұрған ОЖ-ға қарамастан басқа ЭЕМ-ға оңай көшірілуі мүмкін. Осылайша, Web-серверді бір жабдықтан екіншісіне ауыстыру кезінде жүйелік әкімшінің міндеті әлдеқайда жеңіл болады.
2. Мәтіндік форматтағы ақпарат салыстыруға өте қолайлы. Көптеген әкімшілер өздерінің конфигурациялық файлдарын әр өзгерістердің алдында сақтап отырады. Linux және басқа да ОЖ-да пайдаланушы (әкімші) үшін қолайлы түрде әр алуан мәтіндік файлдарды салыстыруға мүмкіндік беретін көптеген бағдарламаларды табуға болады.
3. Мәтіндік пішіндегі конфигурациялық файлдарды кез келген мәтіндік редакторлар, соның ішінде консольдықтар оңай редакциялайды, бұл байланыс жылдамдығымен төмен қашықтан басқару үшін өте пайдалы.
4. Мәтіндік файлдарда конфигурация түсіндірмелер жасауға мүмкіндік береді, бұл белгілі бір баптаулардың мақсаттарын түсінуді жеңілдетеді. Бұған қоса, кейбір конфигурация фрагменттерін оларды түсіндіру арқылы уақытша жою мүмкін болады. Мұндай конфигурация фрагменттері жолдың басынан түсініктеме таңбаларын жою арқылы қалпына келтіруге болады.

Түпкілікті директория. Apache-де *DocumentRoot* директивасымен берілетін түпкілікті директория немесе құжаттардың түпкілікті директориясы деген ұғым бар. Бұл директива сұраныс кезінде пайдаланушыға көрсетілетін мәліметтер файлдары сервердің файлдық жүйесінің қай жерінде сақталатынын көрсетеді. Бастапқыт орнату

бойынша (Alias* директиваларымен лақап аттарды көрсетілмеуінсіз) пайдаланушылық сұранысты алған кезде браузер мекенжайы жолында көрсетілген барлық жол пайдаланушы сұрап отырған ресурсты табу үшін осы түпкілікті директорияға жазылады.

DocumentRoot директивасын соңына бөлшек сызығын қоймай көрсеті керек, мысалы:

```
DocumentRoot "/usr/web"
```

Осылайша, http://my.example.com/index. html мекенжайы бойынша сұраныс Apache серверінің */usr/web/index.html* жолында оның файлдық жүйесінде тұрған құжатты беруіне алып келеді.

DocumentRoot директивасы виртуалдық хостинг кезінде көп рет кездесуі мүмкін (бұл жөнінде бұдан әрі толығырақ айтылады). Әлдеқайда жаһандық директива да бар, ол — *ServerRoot.*

ServerRoot директивасы өз кезегінде бүкіл Web-сервер орнатылған директорияны көрсетеді. Бұған дейін көрсетілген жағдайда бұл директория */home/user/httpd.*

Егер, *DocumentRoot* директивасы абсолюттік емес жолмен көрсетілген болса, онда ол *ServerRoot* директивасы мәніне салыстырмалы болып саналады.

Конфигурация файлында былай деп жазылса да:

```
ServerRoot "/home/user/httpd"

DocumentRoot "web"
```

Бұл мына мәнге тең:

```
DocumentRoot "/home/stud/web"
```

ОЖ қорғаныш жүйесімен өзара әрекеттестік. Әдетте, Әдетте, Apache Web-сервері артықшылықты емес пайдаланушының атынан іске қосылады. Бұл серверді өзіндік қателерінен немесе оған орнатылған бағдарламалардағы қателерден қосымша қорғауға мүмкіндік береді. Apache Web-сервер соның атынан қосылған пайдаланушы үшін қол жетімді емес файлдарды пайдалана алмайтынын есте сақтау қажет.

Осымен бірге Apache-де жарияланған әрбір директорияда өзіндік жеке рұқсаттар бар (1.10-бөлімшені қараңыз).

Қарапайым сайт баптаулары.

Настройка простейшего сайта. Директорияда *conf*— файл *conf/httpd. Conf* орнатқаннан кейін сайттың негізгі баптаулары бар болады. Қарапайым пайдаланушылар (супер пайдаланушылар емес) артықшылықты порттармен (1 024-тен аз) жұмыс істей алмайды,

сондықтан, серверді тыңдау портын өзгерту қажет. Мысал үшін оған 1080 портын тағайындайық.

Сервер үшін порт белгілеуге *Listen* директивасы жауап береді.Оны *httpd. Conf* файлында келесідей үлгіде өзгертуге болады:

```
Listen1080
```

Бұл директива көп рет көрсетілуі мүмкін екеніне назар аударыңыз, бірақ, қарапайым пайдаланушы атынан серверді іске қосу үшін конфигурациялық файлда жазба болмауы қажет

```
Listen80
```

Осыдан кейін *httpd*: bin/httpd-X іске қосуға болады

Опция — X ретке келтіру тәртібінде серверді іске қосады. Бағдарлама аяқталмай жұмыс істеуін жалғастыруы керек. Оның жұмысын браузер арқылы тексеруге болады, яғни, *http://localhost: 1080/* ашып немесе *curl* бағдарламасымен:

```
user@machine:~/httpd> curl 127.0.0.1:1080 <html><body><h1>It
works!</h1></body></html>
```

Егер, үлгі сайт браузер арқылы ашылмаса немесе *httpd* Web -сервері іске қосылмаса, Web-серверді іске қосу және диагностикалауға арналған келесі бөлімдерге жүгіну керек. *Curl* жауабы мынандай болуы мүмкін:

```
user@machine:~/httpd> curl 127.0.0.1:1081 curl: (7) couldn't
connect to host
```

Бұл кезде қандай да бір HTML тегтер болмайды. Бұл қатені Web-сервер емес, Web-серверге қосыла алмаған консольдік браузер қайтарғанын білдіреді.

Web-сервер журналдарында бұл оқиға ешқандай түрде көрсетілмейді, себебі, сұраныс Web-серверге жеткен жоқ және ол сұраныс жүзеге асырылғаны туралы еш ақпарат алмаған.

Егер, мүлде жоқ URL сұрайтын болса, онда Web-сервер HTML кодын түрлендіретіні және ол пайдаланушыға қайтатынын көруге болады:

```
user@machine:~/httpd> curl 127.0.0.1:1080/non-ex-dir/ <!DOCTYPE HTML PUBLIC
"-//IETF//DTD HTML 2.0//EN"><html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
```

The requested URL /non-ex-dir/ was not found on this server.
</body></html>

access_log журналының файлында мұндай сұраныс келесі жазба түрінде көрсетілетін болады:

127.0.0.1 - - [10/Apr/2014:12:37:24 +0400] "GET /non- ex-dir/ HTTP/1.1" 404 209

Мұнда *127.0.0.1* — клиенттің (Web-серверге қосылу орындалған компьютердің) IP-мекенжайы*; 10/Apr/2014:12:37:24 +0400* — дақосылу уақыты (соңғы өрісте сағат белдеуінің көрсетілуімен); *"GET/non-ex-dir/ HTTP/1.1"*— сұраныс мәтіні (HTTP хаттамасына сәйкес). Мұнда GET әдісі қолданылғаны, */non-ex-dir/*жолы сұралғаны және HTTP нұсқасының хаттамасы қолданылғаны көрінбейді1.1; 404 — HTTP мәртебесінің коды, 404 ресурс серверде табылмағанын көрсетеді.

Конфигурацияның қарапайым файлының негізгі бөліктерін қарастырып көрейік:

ServerRoot "/home/user/httpd"

Бұл директива Web-сервердің бағдарламалық қамсыздандыруы орнатылған директорияны белгілейді. Бұдан әрі директорияларға қолжетімділік хабарландырулары келтіріледі. *Directory* директивасындағы директориялар — Web-сервер ашылған сервердің файлдық жүйесінің директориясы:

<Directory />
AllowOverride none
Require all denied </Directory>

Осылайша, бұл баптау сервердің түпкілікті директориясындағы файлдарға қандай да бір қолжетімділікке тыйым салады:

DocumentRoot "/home/user/httpd/htdocs"

Мұнда жарияланатын сайт үшін түпкілікті болатын директория белгіленеді:

<Directory "/home/user/httpd/htdocs">
Options Indexes FollowSymLinks
AllowOverride None Require all granted </Directory>

Конфигурация файлының бұл бөлігінде сайттың түпкілікті директориясына арналған баптаулар белгіленеді. Нақты параметрлер одан әріде келтірілген.

Өнімділікті ұлғайту. Apache екі негізгі тәртіпте жұмыс істей алады: көп процестік (pre-forked, multi-process) және көп ағынды (multi-threaded).

Көп процестік тәртіпте Apache пайдаланушылық сұраныстарға қызмет көрсетуге арналған көп поцестерді іске қосады. Көп процестік тәртіпте Apache ағындардың әрқайсысы пайдаланушылық сұраныстарға қызмет көрсететін бір процесті (кейде көп процесті) іске қосады. Осылайша, егер, серверге 20 пайдаланушылық сұраныс келетін болса, онда көп процесті сервер 20 жаңа процесті іске қосады, ал көп ағынды болса өзінің бір ғана процесінің ішінде 20 жаңа ағынды іске қосады.

Қос әдістің артықшылықтары мен кемшіліктерін қарастырып көрейік.

Көп ағынды нұсқа, әдетте, жылдамырақ және жадыны көп талап етпейді. Дәл сол уақытта, Apache-ге қосылатын қосымша модульдер көпағынды орындауды толық қолдауы керек. 100% ағын қауіпсіздігі жоқ модульдер қателерге немесе Apache серверінің болжап білмейтін жұмысына алып келуі мүмкін.

Көп процесті нұсқа көбірек жадыны талап етеді. Процестерде көп ағындылық пен модульдер жоқ, оны толықтай қолдамайтындар мұндай ортада еш кедергісіз жұмыс істей алады.

Apache үшін ең танымал модульдердің бірі — PHP — оның көпағындылықпен бірқатар проблемалары бар. Егер, нақтырақ айтар болсақ, PHP ядросының модулінің өзі көп ағынды тәртіпте толыққанды жұмыс үшін әзірленген, алайда, осы модуль қолданатын кейбір кітапханалар ағын қауіпсіздігі жоқ. Бұл Apache-ні көп процесті тәртіпте қолдану қажеттілігіне алып келеді.

Көппроцесті модуль (Multi-ProcessingModule) Web-сервердің аз ағынды көппроцесті жұмысын жүзеге асырады. Әрбір серверлік процесс кіріс сұрауларына жауап береді және басты процесс осындай процестердің біршамасын басқарады.

Көп процестік модуль автоматты түрде реттемелетін болып табылады және оның конфигурация директиваларын өзгерту қажеттілігі өте сирек туындайды. Олардың ішіндегі ең маңыздысы — MaxRequestWorkers— айтарлықтай үлкен мәнге орнатылуы керек, себебі, бұл тіпті өте кішкентай сұраныстарға қызмет көрсетуі және ЭЕМ ресурстарын шамадан тыс шығындамауы керек.

Бір ғана бақылаушы процесс қосылуды күтіп тұрған еншілес процестердің іске қосылуына жауап береді және олар пайда болған кезде, оларға қызмет көрсетеді.

Apache барлық кезде бірнеше процесті күту күйінде ұстап тұруға тырысады, бұл оларды кіріс сұраныстарына бір сәтте қызмет көрсету үшін жасалады. Бұл жағдайда клиенттерге жаңа қызмет көрсету процесі құрылуын күтпесе де болады.

*StartServers, MinSpareServers, MaxSpareServers*и *MaxRequestWorkers*

директиваларын бас процестермен қанша еншілес процесс туындауына байланысты күйге келтіріледі. Apache сервері өзін өзі жеткілікті түрде жақсы реттемелейді және бұл директивалар бастапқы орнатудағы мәндері күйінде қалдырылуы мүмкін. Бір уақытта 256-дан астам сұранысқа қызмет көрсету қажет болатын сайттар үшін *MaxRequestWorkers* мәнін ұлғайту қажет. Жады бойынша қатаң шектеулері бар сайттар үшін керісінше, оны кеміту қажет.

UNIX-тектес ОЖ-дегі бас процесс, әдетте, 80 порт ашу мүмкіндігіне ие болу мақсатында супер пайдаланушы атынан іске қосылады. Еншілес процестер, бұл ретте, артықшылығы аз пайдаланушымен іске қосылады.

MaxConnectionsPerChild директивасы ол тоқтатылуы және оның орнына жаңасы іске қосылғанға дейін орындауы тиіс сұраныстардың санын анықтау үшін қолданылады.

Ресурстар жоғалтуды шектеу. Көп процестік тәртіпте іске қосу кезінде Apache-де ресурстар шығынын шектейтін көптеген директивалар бар. Мысалы, егер, іске қосылатын модульдерде жадының жоғалуы орын алса, бұған дейін сипатталғандай еншілес процесс «өлген» кезде жады босатылады. *MaxConnectionsPerChild* мәнінің азаюы жадының жоғалуын азайтады, себебі, олар жиі босатылып тұрады. Apache-де жадыны қолдауды шектейтін кіріктірілген құралдар жоқ. Алайда, UNIX-тектес ОЖ-де *ulimit*командасын қолдануға болады. Командалар синтаксисі мынандай:

ulimit [-acdfHlmnpsStuv] [limit]

Қолжетімді опциялар:

- —*a*— барлық әрекет етуші шектеулерді шығару;
- —c — ядроның құрылатын файлдарының максималды көлемі;
- — *d*— мәліметтер сегментінің максималды көлемі;
- — f— құрылатын файлдардың максималды көлемі (бұл опция бастапқы орнатулар бойынша қолжетімді);
- — H— өрсетілген ресурстар үшін қатаң шектеулер орнату;
- —1 — жадының бұғатталған өрісінің максималды көлемі;
- — *m*— жадыдағы максималды көлем;
- — *n*— дескрипторлардың ашық файлдарының максималды саны;
- — p— кіру-шығу ағыны буферінің көлемі (pipe);
- — *s*— стектің максималды көлемі;
- — *S*— көрсетілген ресурстар үшін жеңіл шектеулер орнату;
- — *t*— процессорлық уақыттың секундтардағы максималды саны;
- — *u*— бір пайдаланушыға арналған процестердің максималды саны;
- — *v*— процесс үшін қолжетімді виртуалды жадының максималды саны.

Ulimit командасы бағдарламалық тысқа және сол арқылы іске қосылған барлық бағдарламалар үшін қолжетімді ресурстарды бақылауға мүмкіндік береді. Соңғы кілт (— v) жады тұтынуын шектеу үшін қолданылуы мүмкін:

```
ulimit -v1048576
```

Мұндай жол процеске 1 Гбайт жады ұсынады. Бұл команданы Apache іске қосу скриптінің соңына жалғау жеткілікті.

Бірнеше серверлерді қолдану. Web-серверлердің мүмкіндіктерін арттырудың бір нұсқасы кластерге бірнеше серверді біріктіру болып табылады, бұл кластер мүшелерінің арасында жүктемені бөлуге мүмкіндік береді. Мұндай әдіс жүктемені теңестіру деп аталады. Apache-де бұл қызметті *mod_proxy_balancer* модулі атқарады. Атауынан көрініп тұрғандай, ол прокси сервер қағидасы бойынша жұмыс істейді. Бұл модульді іске қосу үшін, сондай-ақ, *mod_proxy модулін іске қосу қажет болады. Теңестіру* HTTP, FTPи AJP13 хабарламалары бойынша сұраныстарды қайта бағыттау арқылы жүзеге асырылады.

Жүктемені бөлудің түрлі алгоритмдері бар. Олар жекелеген модульдерде іске асырылған: *mod_lbmethod_ byrequests, mod_lbmethod_bytraffic, mod_lbmethod_bybusyness* және *mod_lbmethod_heartbeat.* Осылайша, жүктемені бөлудің жұмыс істеуі үшін осы модульдердің жоқ дегенде біреуі жүктелуі керек.

Қазіргі уақытта жүктемені бөлудің үш негізгі алгоритмі бар: сұраныстар саны, трафик көлемі және кезек ұзындығы. Алгоритм теңдестіруге арналған *lbmethod* директивасымен анықталады.

Жүктемені тарату серверге клиенттің тіркелуін қолдайды: жүктемені бөлу серверіне қайталанған сұраныс келген кезде, ол алдыңғы уақытқа бағытталған кластердің бір мүшесіне қайта бағытталады. Көптеген алгоритмдер клиенттерді және серверлерді салыстыру түріндегі кесте ретінде осы тәсілді іске асырады. Қосылуды серверлер мен клиенттердің көруі мүмкін емес, бірақ, кейбір проблемаларға алып келеді: егер, көптеген клиенттер прокси-сервер арқылы жұмыс істейтін болса, кластер мүшелерінің арасында сұраныстарды біркелкі емес етіп бөлу мүмкін; сервермен сессия кезінде клиенттің IP-мекенжайының өзгеруі тіркелудің жоғалуына алып келуі мүмкін.

Осы проблемаларды басшылыққа ала отырып, *mod_proxy_balancer* Cookie негізіндегі тіркелуді жүзеге асырады.

Жүктемені бөлудің қарапайы конфигурациясын қарастырайық:

```
<Proxy balancer://mycluster>
        BalancerMember http://192.168.1.50:80 BalancerMember
```

```
http://192.168.1.51:80</Proxy>
ProxyPass /test balancer://mycluster ProxyPassReverse /test
balancer://mycluster
```

/test мекенжайы бойынша келген сұраныстар *balancer://mycluster* теңестірушісіне жіберіледі. Бұл теңестіруші екі мүшеден тұратын кластер деп аталады.

Mod_header модулі көмегімен серверге шығарылатын Cookie көмегімен бекітуді қолдана отырып жүктемені теңестірудің тағы бір мысалы:

```
Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ ROUTE}e;
path=/" env=BALANCER_ROUTE_CHANGED <Proxy balancer://mycluster>
        BalancerMember http://192.168.1.50:80 route=1 BalancerMember
http://192.168.1.51:80 route=2 ProxySet stickysession=ROUTEID </Proxy>
ProxyPass /test balancer://mycluster ProxyPassReverse /test balancer://mycluster
```

Мұнда клиенттің әрбір сессиясына серверге бекіту бағдарын сәйкестендіретін, яғни, кластер мүшесін сәйкестендіруші, Cookie-ауыспалы *ROUTEID* қосылады.

Теңестіруді басқару. Сонымен қатар, теңестіруді басқару қызметі бар. Оның жұмысы тек *mod_status* модулімен ғана мүмкін. Теңестіруді басқару модулі кластер мүшелерін динамикалық түрде өзгертуге мүмкіндік береді. Кластер мүшелерінің кейбір параметрлерін (мысалы, жүктеме салмағын) немесе оның күйін (қосу немесе сөндіру) өзгертуге болады.

Осылайша, осы модулдің жұмыс атқару мүмкіндігі үшін Apache-де бірден *mod_status* және *mod_proxy_balancer* модулдерін қосу қажет.

Браузерден теңестіру параметрлерін өзгерту мүмкіндігін іске қосу үшін келесі конфигурацияны қолдануға болады:

```
<Location /balancer-manager>
        SetHandler balancer-manager Require host
example. com </Location>
```

Содан соң, URL бойынша теңестіруді басқаруға мүмкіндік алуға болады, мысалы, *http://your. server. name/balancer-manager*.

Бекітушілікке қатысты ескертулер. Cookie негізінде серверге бекітушілікті қолдану кезінде сессияға қызмет ететін кластер мүшесі туралы ақпарат бар Cookie атын баптау қажет. Ол үшін *stickysession* атрибуттары, *ProxyPass* немесе *ProxySet*директивтері пайдаланылады. Айнымалы Cookie-дің атауы тіркелімге сезімтал. Бағдарлауыш (*mod_proxy_ba- lancer* модуль бөлігі) Cookie-дан бағыт сәйкестендіргішін

ажыратады және кластер мүшелері арасынан осындай бағыт сәйкестендіргіші бар серверді іздейді.

Кейбір қызмет көрсетуші серверлер сессияны серверге бекіту үшін өзге амал қолданады. Мысалы, Apache Tomcat сессиясы бар Cookie соңына нүктемен бөлінген Tomcat сервер атауын қосады. Осылайша, бағыттауыш ола жақтан серсвер сәйкестендірушісін мүшеліктен шығару үшін *Tomcat* атты Cookie сессияларын табуға тырысады. Tomcat-та сервердің белгілі бір сәйкестендіргішін белгілеу үшін *conf/ server. Xml* файлының құрамын өзгерту қажет.

Сессияны бекітудің тағы бір басқа әдісі — URL кодтау. Бағыттауыш сұраныстан арнайы параметрді іздейді. Бұл параметр дәл сол *stickysession* директивасымен беріледі. Параметр мәні өріс мәні дәл сол *route* болатын кластер мүшесін іздеу үшін қолданылады. URL параметрлерімен әрекеттер тривиалды емес міндет болғандықтан, әдетте, ол соңғы серверге (кластер мүшесіне) жүктеледі. Кейбір жағдайларда *mod_substitute*или *mod_sed* модульдерін қолдана отырып, жүктеме теңестірушісінде орындаған дұрыс. Алайда, бұл сұраныстарды қайта бағыттау жылдамдығына кері әсер етуі мүмкін.

Java стандарттарында URL кодтау біршама өзгеше болып келеді. Олар үтірлі нүктені («;») айырғыш ретінде қолданып, бағыт сәйкестендіргішін URL соңына, ал сессия сәйкестендіргішін үтірлі нүктеден кейін жазады. Cookie жағдаындағыдай, ApacheTomcat осы URL-ге *jvmRoute* мәнін қоса жазуы мүмкін. Сәйкесінше, ApahceHTTPD бұл жолдарды *ProxyPass* немесе *ProxySet* директиваларының көмегімен түсіну үшін сәйкес үлгіде күйге келтірілуі керек.

Cookie атауы мен тік сызықпен жазылған («|»)URL параметрі атауын қолдану арқылы бір уақытта URL-ді кодтау және Cookie-ді қолдануға болады.

```
ProxyPass /test balancer://mycluster stickysession= JSESSIONID|jsessionid
scolonpathdelim=On <Proxy balancer://mycluster>
        BalancerMember http://192.168.1.50:80 route=node1 BalancerMember
http://192.168.1.51:80 route=node2 </Proxy>
```

Егер, бір уақытта Cookie-де де, URL параметрінде де бағыт туралы ақпарат болса, онда URL параметріндегі ақпарат қолданылады.

DNS синонимдерінің қолданылуы. Бір домендік атауы бар көптеген серверлер құру жүктемені бөлудің бір нұсқасы болып табылады. Мысалы, http://www. mail. ru сайты осы қағида бойынша жұмыс істейді.

Мұнда бұл жағдайда барлық IP-мекенжайларға кездейсоқ тәртіпте dns-атауға рұқсат беретін атауларға рұқсат ету кітапханасының ерекшелігі

қолданылады:

```
user@machine:~> host www. mail. ru www. mail. ru has address 217.69.139.70 www.
mail. ru has address 94.100.180.70 user@machine:~> host www. mail. ru www. mail. ru
has address 94.100.180.70 www. mail. ru has address 217.69.139.70 user@machine:~>
ping -c1 www. mail. ru
PING www.mail.ru (94.100.180.70) 56(84) bytes of data.
64 bytes from www.mail.ru (94.100.180.70): icmp seq=1 ttl=58 time=4.60 ms
-----www. mail. ru ping statistics----------
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.609/4.609/4.609/0.000 ms user@machine:~> ping -c1 www.
mail. ru
PING www.mail.ru (217.69.139.70) 56(84) bytes of data.
64 bytes from www.mail.ru (217.69.139.70): icmp seq=1 ttl=58 time=3.95 ms
-----www. mail. ru ping statistics----------
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.959/3.959/3.959/0.000 ms
```

Пайдаланушының браузері сұранысты жолдау үшін IP-мекен-жайы таңдауының дәл сол кездейсоқ алгоритмін пайдаланады. Бұл пайдаланушының барлық сұраныстарын жоғары ықтималдылықпен екі серверге салыстырмалы түрде бірдей бөлуге мүмкіндік береді.

Директориялар индекстерін құру. Файл атауын көрсетпестен сайтты ашу кезінде Apache пайдаланушыға жөнелтілетін файлды таңдап алуы керек. Бұл таңдау *DirectoryIndex* директивасының көмегімен жүзеге асырылады.

DirectoryIndex директивасы клиент директория шіндегіні сұрап жатқан кезде, яғни, сұраныс «/» белгісімен аяқталатын кезде ресурстар тізімін орнатады. Бұл директивада бірнеше мәндер орнатылуы мүмкін. Бұл жағдайда сервер клиентке директорияның бірінші табылған индексін жолдайды. Егер, бірде-бір ресурс табылмаса және *Indexes* директориясының опциясы орнатылған болса, сервер директорияның файлдар тізімін HTML-парақша түрінде әзірлеп, оны клиентке қайтарады:

```
DirectoryIndexindex.html
```

Бұл жағдайда, егер, серверге *http://example. com/docs/* деген сұраныс келсе, ол *http://example. com/docs/ index.html* файлының ішіндегісін қайтарады, егер ол бар болса, әйтпесе, сервер осы директорияның файлдар тізімін қайтарады.

Индекстің файлдар тізімі міндетті түрде қатысты болуы керек месе, яғни, оның құрамында абсолюттік жолдар да болуы мүмкін:

DirectoryIndex index.html index.txt /cgi-bin/index.pl

Бұл жағдайда, егер, сұралған директорияда *index.html*и *index.htm* файлдары табылмаса, */cgi-bin/index.pl* бағдарламасы орындалады.

Жалғыз аргумент *disabled* қолдану индекс файлын іздеуді тоқтатады.

Егер, *disabled* аргументінің алдында және одан кейін тағы қандай да бір аргументтер қойылатын болса, *disabled* файл атауы ретінде қабылданады.

DirectoryIndex көптеген директивалары бір мәнмәтінде ізделіп отырған ресурстар тізіміне қосылады.

Келтірілген мысалда ең алдымен *index.html* файлының, содан кейін — *index.php* файлының іздеуі орындалады:

<Directory/foo>
    DirectoryIndex index.html
DirectoryIndex index.php </Directory>

Келесі мысал алдыңғының әлдеқайда шағын үлгісі болып табылады:

<Directory /foo>
    DirectoryIndex index. html index.php </Directory>

Бұл мысал іздеу үшін ресурстар тізімінің барлық алдыңғы мәндерін қалай жоюға болатынын көрсетеді. Бұл жағдайда *index. Php* іздеуінің ресурсы ғана жүзеге асырылады.

<Directory/foo>
    DirectoryIndex index.html
DirectoryIndex disabled DirectoryIndex
index.php </Directory>

Файлдарға қолжетімділік уақытын шектеу. Сервердегі мәліметтерге қолжетімділікті уақытша шектеу үшін *mod_rewrit* модулін қолдануға болады, ол кейбір талаптар сақталған жағдайда клиенттің сұранысын басқа мекенжайға бағыттауға мүмкіндік береді.

Пайдаланушыларға файлдарға қолжетімділікті 2.00-ден 6.00-ге дейін тоқтату қажет деп санайық. Конфигурация файлына келесі жолдарды қосамыз:

RewriteCond %{TIME_HOUR} ^0[2-5]$
RewriteRule ^.*$!^index\.html$ http://www.example.com/ we-are-closed.html [R=302,L]

Бірінші жол сұранысты қайта бағыттау орындалатын талапты белгілейді. Нақты 2.00.00-ден 5.59.59-ға дейінгі барлық уақыт қамтылуына назар аударыңыз.

Екінші жол сұранысты қайта бағыттау ережесін белгілейді. Бұл жағдайда, индекстік парақшаларға жолданған барлық сұраныстар *http://www. example. com/we-are-closed.html* мекенжайына қайта бағытталатын болады.

Директивалар әрекетінің аясын шектеу. Негізгі конфигурациялық файлда орналастырылған директивалар бүкіл серверге таратылады. Директиваны сервердің бір бөлігіне ғана қолдану қажеттілі кезінде ол директиваларды <Directoiy>, <DirectoiyMatch>, <Files>, <FilesMatch>, <Location>*и*<LocationMatch> тегтерінің ішіне орналастыру қажет. Бұл тегтер оларда көрсетілген директиваларды файлдық жүйенің белгілі бір директорияларына немесе URL жолдарына қолдануын шектейді. Бұл тегтер бір-бірімен капсулдануы мүмкін, бұл Web-сервердің түрлі бөліктерінің икемді және қарапайым баптауларын құруға мүмкіндік береді.

Apache бір уақытта бірден бірнеше сайттарға қызмет көрсете алады. Бұл виртуалды хостинг деп аталады. Директивалар <VirtualHost> тегінің ішінде көрсетілуі мүмкін, осылайша олар тек осы виртуалды хостқа ғана қолданылады.

Көптеген директивалар түрлі тегтерде орналастырылуы мүмкін екеніне қарамастан, олардың кейбірі еленбеуі мүмкін. Apache құжаттамасында әрбір директиваның сипаттамасында ол қайда қолданылатыны жазылған. Мысалы, клиенттер сұраныстарына қызмет көрсету процестерін құруды бақылаушы директивалар конфигурациялық файлдардың негізгі аумағында (тегтерден тыс) орналастырылу ымүмкін.

Конфигурацияны резервтеу. Веб-сервердің бүкіл конфигурациясы мәтіндік файлда екендігін ескере отырып, оны сақтау айтарлықтай ыңғайлы. Өзгерту кезінде сақтаудың келесі сяасаты жиі қолданылады. Сәтті жұмыс істейтін Web-серверді қайта баптау қажет болған кезде, өзгертілетін файлдарды суффиксі бар – өзгеру уақыты бар резервтік көшірмелер түрінде сақтайды. Мысалы, *httpd. conf* файлын 2004 жылдың 3 сәуірінде өзгерткен. Онда директориядағы файлдар келесідей үлгіде болады: httpd.conf
httpd.conf.2004-04-03

Күнделікті көптеген өзгертулер кезінде өзгерту нөмірі бар суффиксті қосуға болады:

httpd.conf
httpd.conf.2004-04-03-01
httpd.conf.2004-04-03-02
httpd.conf.2004-04-03-03

Бұл тәсіл өзгерістерді уақыт бойынша қадағалауға мүмкіндік береді. Көптеген конфигурация қателері ұзақ уақыт өткен соң ғана анықталуы мүмкін. Мұндай жағдайларда қандай да бір өзгертулер қашан енгізілгенін білу қажет.

Мәтіндік файлдар көптеген мәтінді өңдеу құралдарымен салыстыруға және талдауға оңай салынады. Мұнда *httpd. conf* файлын алдын ала резервтіп алып, оны өзгерту ғана қажет. Мысалы, тыңдау портын 1080-нен 1088-ге дейін ауыстырып қосу керек. Өзгертулерді *diff* командасының көмегімен көрсетуге болады:

```
user@machine:~/httpd-install/conf> diff httpd.
conf.2013-02-01 httpd. conf
52c52

< Listen 1080 > Listen 1088
```

Өзгертілген жолдардан бөлек тағы басқа мәнмәтін бар біркелкіленген diff-файл әлдеқайда қолайлы болуы мүмкін:

```
user@machine:~/httpd-install/conf> diff -u httpd. conf.2013-02-01 httpd. conf
----- httpd.conf.2013-02-01 2014-01-31
12:12:34.000000000 +0400
+++ httpd. conf 2014-02-11 11:52:50.554984341 +0400 @@ -49,7 +49,7 @@
     # prevent Apache from glomming onto all bound IP addresses.
     #
     #Listen 12.34.56.78:80 -Listen 1080 +Listen 1088
 #
 # Dynamic Shared Object (DSO) Support
```

Бұл түрде өзгертілген жолдың өзі неге қатысты екенін түсіну оңайырақ, себебі, өзгеріске дейінгі және өзгерістен кейінгі жолдардың үш жолдарынан келтірілген.

Барлық әкімшілерге алуан түрлі болжап білмейтін жағдайлардан сақтану үшін өздерінің барлық серверлерін автоматты резервтеуді жүргізу ұсынылады: қатты дисктің істен шығуынан сервер орналасқан ғимараттан өрт шығуына дейінгі жағдайлар.

1.7. СЕРВЕРДІ ҚОСУ, ҚАЙТА ҚОСУ ЖӘНЕ ТОҚТАТУ

Сервермен операциялар үшін bin/httpd бағдарламасы қолданылады. Ол сервердің негізгі атқарушы модулі болып та, сервмермен «әңгімелесуге» арналған команда болып та табылады.

Іске қосылғаннан кейін бұл бағдарлама демон тәртібіне көшеді:

```
user@machine:~/httpd-install/bin>  ./httpduser@machine:~/httpd-
install/bin>
```

Демон тәртібінде іске қосу – UNIX тобындағы ОЖ қатарында әзірленген серверлер үшін жалпымен қабылданған қалып болып табылады. Бұл іске қосылған процесс *fork()* жүйелік шақыруының көмегімен тағы бір процесті тудырады дегенді білдіреді. Іске қосылған еншілес процесс ағымдағы терминалдан босатылып, аялық тәртіпте орындала бастайды. Осы уақытта бас процестің жұмысы аяқталады да, ол командалық жолдың шақыруы бойынша тәмамдалады.

Командалық жолдың параметрлері бойынша анықтама алу үшін Web-сервердің *man* үлгісіндегі стандартты құжаттамасын қолдануға болады:

```
man8 httpd
```

Оның демонын ек рет іске қосуға болмайтынына назар аударыңыз:

```
user@machine:~/httpd-install/bin>  ./httpd  user@machine:~/httpd-
install/bin> ./httpd httpd (pid 22710) already running
```

Осылайша, *httpd* командасы іске қосылып қойған *httpd* демоны жайлы расында да білетінін көруге болады. Мұны демонға кейбір командаларды жолдау үшін қолдануға болады. Құжаттамада бұл келесідей үлгіде жазылған:

```
-k start|restart|graceful|stop|graceful-stop Signals httpd to start, restart, or stop.
SeeStoppingApacheformoreinformation.
```

Ендеше, параметрді — *к* демонды тоқтату, қосу және қайта қосу үшін қолдануға болады. Демонды тоқтатып, оны тағы да қосып көрейік:

```
user@machine:~/httpd-install/bin> ./httpd -kstopuser@machine:~/httpd-install/bin>
./httpd -kstart
```

Команданың сәтті орындалуы консольге қосымша ақпарат шығармайтынына назар аударыңыз, ал сәтсіз орындалу қосымша түсіндірулермен жабдықталады:

```
user@machine:~/httpd-install/bin> ./httpd -k start httpd (pid 23157) already running
user@machine:~/httpd-install/bin> ./httpd -k stop user@machine:~/httpd-install/bin>
./httpd -k stop httpd (no pid file) not running
```

Соңғы хабарламадан демон сәйкестендіруі үшін PID-файл (PID—processidentifier) *httpd* қолданатыны түсінікті. PID-файл – бұл сонымен қатар жалпымен қабылданған техника. Демонды іске қосу кезінде ол демон процесінің идентификаторы жазылатын файл құрады. Осылайша, егер, тағы бір демон іске қосқысы келсе, ол PID-файлдың бар-жоғын тексереді. Егер, файл бар болса, онда одан демон процесінің идентификаторы алынады және одан әрі демонмен байланыс арнасы ашылады.

ApacheHTTPServer жағдайында PID-файлдың орналасқан орны конфигурация файлындағы *PidFile* директивасымен анықталады. Бастапқы орнату бойынша PID-файл *logs/httpd. Pid* директориясында болады. Егер, файлға арналған жол бастапқы бөлшек сызықсыз көрсетілген болса, онда ол демонды орнату директориясынан саналады.

Apache-ні іске қосып, процесті тексерейік:

```
user@machine:~/httpd-install> cat logs/httpd.pid 23541
user@machine:~/httpd-install> cat /proc/23541/cmdline ./httpd-
kstartuser@machine:~/httpd-install>
```

Соңғы жолдың басында демонды іске қосудың командалық жолы шығарылған. Барлық бос орындар қалдырылған. Бұл ОЖ-ның командалық жолының ішкі ұсынылуымен байланысты. Ол барлық параметрлерді NULL-terminatedstrings түрінде сақтайды, яғни, барлық парамтерлер бір-бірінен NULL таңбасымен немесе 0 коды бар таңбамен бөлінген. Бұл таңба консольге шығарылмайды. Алайда, sed ағындық редакторының көмегімен бос орынға ауыстыруға болады. Пайдаланушының келесі шақыруынан бөлу үшін шығарудың соңына *echo* командасын қосамыз:

```
user@machine:~/httpd-install>cat /proc/23541/cmdline | sed "s/\x0/ /g"; echo ./httpd -k
start
```

Серверді қайта іске қосу үшін *stop* және *start* қос командасының орнына *restart* командасын қолдануға болатыны айдан анық түсінікті. Алайда, *restart* командасын орындау кезінде демон PID-і өзгермейді, сәйкесінше, демон тоқтамайды, ол тек барлық конфигурацияны қайта есептейді де, басынан бастап іске қосылады. Бұл процесті қосу мен тоқтату ресурстардың айтарлықтай көлемін қамтитын үлкен серверлік шешімдер үшін қолайлы болады.

Apache жұмыс ыңғайлылығы үшін *httpd— к* ұқсас, басқарушы командалардың жөнелтілуін жүзеге асыратын *apachectl* файлын ұсынады. Осы команданың көмегімен серверді, тоқтату, қосу және қайта қосу келесідей үлгіде мүмкін болады:

user@machine:~/httpd-install> bin/apachectl start user@machine:~/httpd-install> bin/apachectl stop user@machine:~/httpd-install> bin/apachectl restart

MacOS ОЖ атынан іске қосу. MacOS атынан іске қосу Linux атынан іске қосуға ұқсас жүзеге асырылады, бұл аталған ОЖ-лар бір топқа жататынымен түсіндіріледі. Іске қосу үшін */Applications/Utilities/Terminal* терминалын ашу қажет. Терминалда жоғарыда сипатталғандай *apachectl* командасы қолжетімді болады. Бастапқы орнатулар бойынша Apache жүйелік бағдарламалық қамсыздандыру ретінде орнатылған және сол себепті басқару үшін супер пайдаланушы артықшылығын талап етіп отыр.

Apache күйін басқару үшін терминалда келесі командалар қолданылады:

sudo apachectl start sudo apachectl
stop sudo apachectl restart

Windows ОЖ атынан іске қосу. Windows ОЖ басқаруында Apache жүйелік қызмет ретінде іске қосылады. Бұл опция Apache орнату кезіндегі процесте қолжетімді.

Windows-ке арналған Apache жинағына ApacheServiceMonitor (Apache қызметінің мониторы) атауы бар утилита кіреді. Оның көмегімен пайдаланушы Apache-нің барлық орнатылған серверерінің жағдайын басқара алады. Бұл бағдарламаны пайдалану үшін Apache-ні жүйелік қызмет ретінде алдын ала орнату қажет.

Қызмет ретінде Apache орнату үшін оны орнатудың негізгі директориясындағы *bin* директориясынан *httpd. exe* командасын қолдану керек:

httpd.exe -kinstall

Қызмет ретінде орнатқан кезде келесі команданы пайдаланып, қызметтің атын көрсетуге болады:

httpd.exe -k install -n "MyServiceName"

Бұл бір ЭЕМ-де бірнеше Apache серверлерін орнату кезінде пайдалы болуы мүмкін. Бұл қызметтің атауы орнату кезінде көрсетілуі мүмкін, бірақ, кейінірек ол к - опциясы үшін команда жолында параметрмен көрсетілуі мүмкін.

Қажет болған жағдайда орнатылатын қызмет үшін сонфигурацияның

нақты файлы көрсетілуі мүмкін:

```
httpd.exe -k install -n "MyServiceName" -f "c:\files\ my.conf"
```

Егер, қызмет атауы көрсетілмесе, автоматты түрде *Apache2.4* (немесе нұсқасына байланысты басқа атау) атауы беріледі. Бастапқы орнатулар бойынша конфигурация файлы *conf\httpd. conf* қолданылады.

Apache қызметін жою дәл сол команданың көмегімен орындалады:

```
httpd.exe -kuninstall
```

Apache-дің белгілі бір қызметін де жоюға болады:

```
httpd.exe -k uninstall -n "MyServiceName"
```

Apache серверінің штатық қосуы, тотатуы және қайта қосуы, әдетте, мына командаларды қолдана отырып, ApacheServiceMonitor арқылы жүргізеді:

```
net start Apache2.4 net stop
Apache2.4
```

Сондай-ақ, Apache қызметтерін стандартты Windows қызмет басқару интерфейсі арқылы басқаруға болады. Apache қызметін іске қоспас бұрын, конфигурация файлының дұрыстығын мына команданың көмегімен тексеру ұсынылады:

```
httpd.exe -n "MyServiceName" -t
```

Apache қызметін *httpd. exe* командасының көмегімен басқаруға да болады:

```
httpd.exe -k start -n "MyServiceName" httpd.exe -k stop -n
"MyServiceName" httpd.exe -k restart -n "MyServiceName"
```

Ретке келтіру тәртібі. Жиі жағдайда консольде сервермен шығарылатын барлық ақпаратты консольде көру үшін серверді ретке келтіру тәртібінде іске қосу керек. Мұндай іске қосу арнайы параметрдің көмегімен жүзеге асырылады:

```
user@machine:~/httpd-install/bin> ./httpdX
```

Бұл тәртіп серверді ретке келтіру үшін қолданылады. Конфигурция мен орнатылған модульдерді ретке келтіруге мүмкіндік берілетін сервердің бірағынды тәртіпте іске қосылуы аталған тәртіптің басты ерекшелігі болып табылады.

1.8. БІРНЕШЕ WEB-ТОРАПТАРДЫҢ ХОСТИНГІ

Замануи серверлердің есептеуіш қуаты айтарлықтай үлкен және бір серверге бірнеше сайт орналастыру қатардағы міндеттің бірі болып қалды. Бұл электр қуаты, жабдық құны және IP-мекенжайларды жалға алу мәселесінде үнемдеуге мүмкіндік береді. Хостинг-провайдерлердің басым бөлігі дәл осы тәртіпте олардың серверлерінде сайттарды орналастыру қызметтерін ұсынады.

Apache терминологиясында бұл технология виртуалды хостинг (VirtualHosting) деп аталады. Web-сервердің бағдарламалық қызметі клиент браузерінен сұраныс алып, пайдаланушымен қандай виртуалды торап сұралып отырғанын анықтайды және осы виртуалды тораптар сайт ұсынады.

IP-мекенжайлар мен порттар бойынша бөлу. Виртуалды хостингтің ең қарапайым нұсқасы – IP-мекенжайлар мен порттар бойынша бөлу. Түрлі IP-мекенжайларды/порттарды тыңдайтын бірнеше Web-серверді іске қосу мұны жүзеге асырудың ең қолайлы әдісі болып табылады. Мысалы, келесі TCP сокеттері бойынша бірнеше сайт орналастыру қажет:

- 192.168.0.100:80;
- 192.168.0.100:88;
- 192.168.0.101:80.

Ол үшін *httpd* үш данасын орнатып, оларды сәйкес конфигурацияларымен іске қосу қажет:

1) */home/user/httpd-1/conf/httpd. conf* Listen

192.168.0.100:80

2) */home/user/httpd-2/conf/httpd. conf* Listen

192.168.0.100:88

3) */home/user/httpd-3/conf/httpd. conf* Listen

192.168.0.101:80

Кейде сайттардың бұл конфигурациясы орынды болуы мүмкін. Дегенмен, көбінесе, төмендегі себептер бойынша процессорлық уақыттың,

қатты магниттік дискі кеңістігі және жадының шығындары артық болады:

1. *httpd* түрлі орнатуларында тұрған файлдардың басым көпшілігі бірдей болады – бұл кітапханалар, құжаттамалар мен қосылатын модульдердің файлдары.

2. Web-серверДІҢ бағдарламалық қамсыздандыруы өзінің ішкі қызметтері үшін орталық процессордың кейбір ресурстары мен жадыны талап етеді. Көлемі шағын сайтты орналастырған жағдайда сервердің ішкі процестерімен тұтынылатын ресурстар көлемі жағынан сайтты сүйемелдеуге қажетті көлемнен асып түсуі мүмкін.

Бұл кемшіліктерге жол бермес үшін виртуалды хостинг техникасы енгізілген. Сонда *httpd* сервердің бір данасы бірнеше сайтқа қызмет көрсете алады. Әрбір жекелеген сайт виртуалды хостингте (виртуалды торапта) орналастырылады.

Виртуалды хост *httpd. conf* конфигурация файлында <VirtualHost> тегімен жазылады. Сипаттаудың қарапайым мысалын қарастырып көрейік:

<VirtualHost 127.0.0.1:80>
ServerAdmin webmaster@mysite. org ServerName
www.mysite.org ServerAlias mysite.org
DocumentRoot /home/user/httpd/htdocs/mysite </VirtualHost>

VirtualHost тегінің жарияланымында осы виртуалды хост байланысты болатын TCP-сокет көрсетіліп тұр. Виртуалды хосттың ішінде виртуалды хостингі жоқ дәл сол сервердің баптауларында қолданылатын барлық баптаулар қолданылуы мүмкін. Осылайша, әрбір виртуалды хосттың *DocumentRoot* сайтының жеке өз бастауы, сайт атауы, жеке өз баптаулары мен әкімшінің электронды поштасының мекенжайлары болады.

Таңдалған виртуалды хост үшін дербес журналдарды баптау да маңызды ерекшелік болып табылады:

ErrorLog /home/user/httpd/logs/mysite-error.log CustomLog
/home/user/httpd/logs/mysite-access. log combined

Осылайша, құрылатын виртуалды хсотқа жатқызылған журналдағы барлық жазбалар *mysite-error* жекелеген файлдарына түсіп отырады. *Log пен mysite-access.log* виртуалды хосттарды әкімшілендіру мен мониторнгін жүргізуді айтарлықтай жеңілдетеді.

Сәкйесінше 8081 мен 8082 порттарын тыңдайтын екі фиртуалды хост үшін конфигурация файлын әзірлейік:

<VirtualHost 127.0.0.1:8081>

ServerAdmin webmaster@mysite. org ServerName www.mysite.org ServerAlias mysite.org
DocumentRoot /home/user/httpd/htdocs/mysite ErrorLog /home/user/httpd/logs/mysite-error. log
CustomLog /home/user/httpd/logs/mysite- access.log combined </VirtualHost>

<VirtualHost 127.0.0.1:8082>
ServerAdmin webmaster@myothersite. org ServerName www.myothersite.org ServerAlias myothersite.org
DocumentRoot /home/user/httpd/htdocs/myothersite ErrorLog /home/user/httpd/logs/myothersite-error. log
CustomLog /home/user/httpd/logs/myothersite- access.log combined
</VirtualHost>

Web-сервер виртуалды хосттарда көрсетілген порттарды тыңдауды бастауы үшін виртуалды хосттар жарияланымдары жеткіліксіз. Сондай-ақ, *Listen* директивасын қосу қажет:

Listen127.0.01:8081
Listen127.0.01:8082

Серверді қайта іске қосу арқылы Web-сервер процесі көрсетілген порттарды расында да тыңдап отырғанына көз жеткізуге болады:

user@machine:~/httpd-install> bin/apachectl restart user@machine:~/httpd-install> netstat -anpt | grep 808 (Not all processes could be identified, non-owned process info will not be shown, you would have to be root to see it all.) tcp 0 0 127.0.0.1:8081 0.0.0.0:* LISTEN 1520/httpd
tcp 0 0 127.0.0.1:8082 0.0.0.0:* LISTEN 1520/httpd

http:// localhost:8081 мекенжайы бойынша қайта құрылған сайтқа кіру әрекеті кезінде пайдаланушы «Forbidden You don't have permission to access / on this server.» қате туралы хабарлама алады. Осы сайттың журналында сұраныс туралы және ққате туралы жазба пайда болады:

user@machine:~/httpd/logs> cat mysite-access.log 127.0.0.1 - - [19/Feb/2014:12:51:40 +0400] "GET / HTTP/1.1" 403 202 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:17.0) Gecko/17.0 Firefox/17.0" user@machine:~/httpd/logs> cat mysite-error.log [Wed Feb 19 12:51:40.226239 2014] [authz core:error]
[pid 5450:tid 139804309366528] [client 127.0.0.1:55432] AH01630: client denied by server configuration: /home/ user/httpd/htdocs/mysite/

Қолжетімділік журналының файлындағы жазба 403 қатесімен (қолжетімділікке тыйым салынған) аяқталған директорияға қолжетімділік туралы «/» хабарлауда. Қателер журналындағы жазба әлдеқайда нақтырақ қате жайында айтуда: сервер баптауларына сәйкес пайдаланушының қолжетімділігіне тыйым салынған.

Қолжетімділіктегі қате *httpd. conf* файлында сайттың орналасу директориясына қолжетімділік ұсынылмауы себептен орын алады — */home/ user/httpd/htdocs/mysite/*. Бұған дейін айтылғандай, сайт ретінде Web-сервермен қолданылатын барлық директориялар *httpd. conf*-қа ретке келтірілуі керек:

```
<Directory "/home/user/httpd/htdocs/mysite">
        Allow from All
        Require all granted
</Directory>

<Directory "/home/user/httpd/htdocs/myothersite"> Allow from All Require all granted
</Directory>
```

Web-сервердегі директориялар мен ресурстарға қолжетімділік ұсынуды алдағы бөлімдерде толығырақ сипатталады.

Сайттардың ашылатынын тексеру үшін сайттар директориясына *index.htmlиз htdocs* көшірмелейміз. Оны браузерде ашуға немесе мына консоль арқылы қолжетімділікті тексеруге болады:

```
user@machine:~/httpd> wget http://localhost:8081/in- dex. html
--2014-02-26 12:07:02-- http://localhost:8081/index. html
localhost (localhost) анықталуда... 127.0.0.1 localhost-ке қосылу
(localhost)|127.0.0.1|:8081... қосылу орындалды.
HTTP-сұраныс жіберілді. Жауа күтілуде... 200 Ұзындығы: 45 [text/html]
Каталогқа сақтау: ""index.html"".

100 %[==============================================
==================================================>]

45        --.-K/s за0s

2014-02-26 12:07:02 (2,66 MB/s) - "index.html" saved [45/45]
```

Сайттарды сәкестендіру үшін *index. html* файлына сайт атауын қосамыз:

- *htdocs/mysite/index.html:*

```
<html><body><h1>It works! (my other site)</h1></body></ html>
```

- *htdocs/myothersite/index. html:*

<html><body><h1>It works! (my site)</h1></body></html>

Сервер атауы бойынша бөлу. Барлық виртуалды хосттардың бір IP-мекенжайда немесе бір портта орналасуы кезінде виртуалды хостингті қолдану қажеттілігі жиі орын алатын жағдай болып табылады. Бұл Интернеттен көрінетін IP-мекенжай ақысы бөлек төленетін қызмет болып табылуымен байланысты болып отыр және әрбір виртуалды хост үшін «аппақ» жаңа IP-мекенжай сатып алу ақталмауы мүмкін. Мұндай жағдайда клиент сервердің қандай атауын сұрап отырғаны негізінде виртуалды хостинг-сервер қандай сайтты беру керек екенін анықтайды. Сервер атауын анықтау үшін сервер атауы тұрған HTTP-сұраныстың басын сканерлеу керек екені белгілі.

Ағылшын тілді әдебиетте бұл техника Name-basedVirtualHosts деп аталады. Apach-нің айтарлықтай ескі нұсқаларында (2.2 және одан да ескі) сервер виртуалды хосттарға арналған сұраныстарды қабылдайтын TCP-сокеттің (IP-мекенжай және порт) тағайындалуының қажеттілігі бар болатын. Бұл *NameVirtualHost* директивасының көмегімен ретке келтірілетін. Apache2.4-те бұл қажет емес.

Сайтты клиентке беру үшін виртуалды хост таңдау кезінде Apache сұраныс келген TCP-сокетіне сәйкес келетін ең қолайлы виртуалды хостты (едәуір ерекше) таңдауға тырысады.

Одан әрі, көптеген бірдей ерекше хосттар табылса, Apache клиент сұраған сервер атауын *ServerName* және *ServerAlias* виртуалды хосттарының директиваларымен салыстырады. Егер, виртуалды хосттар арасында осы директивалар үшін сәйкес келетіні табылмаса, Apache конфигурация файлында сипатталғандардан бірінші *VirtualHost*-ты таңдайды.

Атаулары бойынша виртуалды хостингті жүзеге асыру үшін біздің конфигурация файлымызды түрлендіреміз:

<VirtualHost 127.0.0.1:8081>
ServerAdmin webmaster@mysite. org ServerName www.mysite.org ServerAlias mysite.org
DocumentRoot /home/user/httpd/htdocs/mysite ErrorLog /home/user/httpd/logs/mysite-error.log CustomLog /home/user/httpd/logs/mysite-access.log combined </VirtualHost>

<VirtualHost 127.0.0.1:8081>
ServerAdmin webmaster@myothersite. org ServerName www. myothersite.org

ServerAlias myothersite. org
DocumentRoot /home/user/httpd/htdocs/myothersite
ErrorLog /home/user/httpd/logs/myothersite-error. log
CustomLog /home/user/httpd/logs/myothersite- access.log combined
</VirtualHost>

Браузер *http://www.mysite. org* мекенжайын сұрау кезінде көрсетілген TCP-сокетке жүгінуі үшін необходимо DNS атауларына немесе DNS-серверде не болмаса жергілікті түрде жұмыс станциясында — файлда */etc/hosts* рұқсат ету керек. */etc/hosts* жолдарын қосамыз:

127.0.0.1 localhost mysite. org www. mysite. org myothersite.org www. myothersite.org

Егер, */etc/hosts*-те 127.0.0.1 кілті бар жазба бар болса, онда оның соңына сайттардың қажетті атауларын қоса жазып, оны өзгерту қажет. Өзгерту үшін бұл файлда суперпайдаланушы (root) құқықтары қажет етіледі. Мұндай өзгерту ағымдағы жұмыс станциясындағы DNS-атаулардың рұқсаттарына әсерін тигізеді. *ping* командасымен рұқсаттың жұмыс істеу қабілетін тексерейік:

user@machine:~/httpd/conf>ping -c 1 www. mysite. orgPINGlocalhost (127.0.0.1)
56(84) bytesofdata.
64 bytes from localhost (127.0.0.1): icmp seq=1 ttl=64 time=0.057 ms

----- localhost ping statistics ----------
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.057/0.057/0.057/0.000 ms

dig пен *host* командалары бұл атауға бұрынғысынша рұқсат етпейді, себебі, сұраныстарды тікелей DNS-серверге жолдап отыр, ал */etc/hosts* файлы *libresolve. so* кітапханасының шақырылуына ғана ықпал ете алады:

user@machine:~/httpd/conf> host www.mysite.org www. mysite. org is an
alias for bofh. mysite.org. bofh.mysite . org has address 207.114.175.49

*mysite. org*у домендік атауы Интернетте тіркеліп қойған және белгілі бір IP-мекенжайларға рұқсат етіледі. *Dig* командасы да осы тектес нәтиже береді.

/etc/hosts файлын түрлендіруден кейін қос виртуалды тораптың жұмыс істеу қабілетін тексеруһіп көруге болады:
user@machine:~/httpd/conf> curl localhost:8081 <html><body><h1>It works! (my
site)</h1></body></html> user@machine:~/httpd/conf> curl mysite.org:8081

<html><body><h1>It works! (my site)</h1></body></html>
user@machine:~/httpd/conf> curl www. mysite.org:8 081 <html><body><h1>It works! (my site)</h1></body></html> user@machine:~/httpd/conf> curl www.myothersite. org:8081
<html><body><h1>It works! (my other site)</h1></body></ html>
user@machine:~/httpd/conf> curl myothersite.org:8081 <html><body><h1>It works! (myothersite)</h1></body></ html>

curl командасының қорытындысында көрініп тұрғандай, сайттар ойдағыға сәйкес жүктеледі.

Пайдаланушылардың үй парақшалары. Apache-де пайдаланушылардың арнайы директорияларынан – пайдаланушылардың үй парақшалары - *mod_userdir* ақпарат ұсынатын модуль бар. Ол URL негізінде *http://example.com/~user/* түріндегі әрбір пайдаланушы үшін өзгеше директорияларға қолжетімділікті ұсынады.

UserDir директивасы осы тектес URL-дан ақпарат алу үшін қолданылатын пайдаланушының үй директориясына нақты директория орнатады. Директорияның ішінде мыналар болуы мүмкін:

- директория атауы немесе бұдан әрі көрсетілгендей үлгі;
- *disabled* кілт сөзі. Бұл жағдайда пайдаланушылардың үй парақшаларын ұсыну механизмі сөндіріледі, бұл *enabled* нақты белгіленген пайдаланушыларды есепке алмағанда;
- соңында пайдаланушылардың атаулары көрсетілген *disabled* кілт сөзі. Осы тізімде атаулары шығатын пайдалунышалыр үшін одан әрі қарай осы пайдаланушылар *enabled* опциясында көрсетілсе де модульдің жұмыс істеуі сөндірулі болады;
  - пайдаланушылар атауларының тізімі көрсетілген *enabled* кілт сөзі. Модуль *disabled* сөзімен (бірақ, пайдаланушылардың кейінгі атауларын көрсетпей) сөндірілген болса да, аталған пайдаланушылар үшін модуль қызметі жұмыс істейтін болады. Егер, не *enabled,* не *disabled* көрсетілмесе, *UserDir* директивасының аргументі қайта адрестеу жүзеге асырылуы тиіс үлгі немесе директория атауы ретінде қарастырылады. URL *http://www.example.com/~bob/one/two.html* сұралған болса да. Пайдаланушылар директориясының түрлі мәндері көрсетілген кездегі қайта бағыттауды қарастырайық (1.1-кесте).

1.1-кесте

Директория	Файлды іздеу жолы
UserDir public_html	*~bob/public_html/one/two. html*
UserDir /usr/web	*/usr/web/bob/one/two. html*
UserDir /home//www*	*/home/bob/www/one/two. html*

1.2-кестеде келтірілген жағдайларда клиентке басқа мекенжайға қайта бағыттау жолданады.

1.2-кесте

Директория	Файлды іздеу жолы
UserDir http://www. example. com/ users	*http://www. example. com/users/ bob/one/two. html*
UserDir http://www. example. com//usr*	*http://www. example. com/bob/usr/ one/two.html*
UserDir http://www. example. com/~/*	*http://www. example. com/~bob/ one/two.html*

Бұл директиваның қолданылуына назар аудару қажет. Мысалы, *«UserDir./»* болса «/~root» в «/» бағыттайды, бұл қауіпсіздік мәселесінде қажетсіз болып табылады. *Root* пайдалнушыға қолжетімділікті сөндіру қатаң түрде ұсынылады:

```
UserDirdisabledroot
```

Қосымша тағы бірнеше мысал келтірейік. Бірнеше және одан да басқа ешкімге қолжетімділікті ұсыну:

```
UserDir disabled
UserDir enabled userl user2 user3
```

Нақты белгіленгендерінен басқа пайдаланушылардың барлығына модульге қолжетімділікті ұсыну:

```
UserDirdisableduser4 user5 user6
```

Іздеу үшін балама пайдаланушылық диреткорияларды қолдану:

```
UserDir public html /usr/web http://www.example.com/
```

Мейлі *http://www. example. com/~bob/ one/two. html* мекенжайға

сұраныс келсін. Apache *~bob/public_html/one/ two.htmlfirst* файлын, одан соң *—/usr/web/bob/one/two.html* файлын табуға тырысады және соңында, егер, алғашқы екі файлд да табылмаса, *http://www. example. com/bob/one/two.html* URL-ге қайта бағыттайды.

1.9. ТІРКЕУ ЖӘНЕ МОНИТОРИНГ

Қателерді тіркеу. Web-сервердің жұмысын тиімді баптау және ретке келтіру үшін серверден қандай да бір кері байланыс, сондай-ақ анықталған ақаулар мен оқиғалардың сипаттамасын алу керек. Apache журналдаудың интеллектулды және икемді жүйесін ұсынады.

Web-сервердің жұмысын неғұрлым тиімді баптау және ретке келтіру үшін, серверден қандай да бір кері байланыс, сондай-ақ анықталған ақаулар мен оқиғалардың сипаттамасын алу керек. Apache журналдаудың интеллектуалды және икемді жүйесін ұсынады. Бұған дейін Apache журналдарынан есептеулер ұсынылған болатын. Оларды толығырақ қарастырайық.

Apache сервермен болып жатқан әрекеттердің барлығын журналдаудың түрлі механизмдерін ұсынады: пайдаланушылардың қарапайым сұраныстары мен URL-ді қайта бағыттаудан бастап Apache модульдерінің жұмысында және баптауларында анықталған барлық қателер мен ақпарат берудің соңғы нүктесіне дейін. Қосымша ретінде, шеткі модульдер журналдаудың өз мүмкіндіктерін ұсына алады немесе Apache журналдауының штаттық модульдерін қолдана алады.

ErrorLog директивасында көрсетілген сервер қателерінің журналы (servererrorlog) журналдың өте маңызды файлы болып табылады. Бұл Apache өз диагностикалық ақпараттары мен барлық қателерді жазып отыратын орын. Бұл Web-сервер дұрыс емес жұмыс істеген кезде бірінші тексерілетін орын болып табылады.

Қателер журналы, әдетте, *error_log* файлына жазылады, бірақ, UNIX-жүйелерде *syslog* та қолданылуы мүмкін.

Хабарламалар пішімі қандай мәндер журналдануы керек екенін ретке келтіретін *ErrorLogFormat* директивасымен сипатталған. Бастапқы орнатулар бойынша пішім, егер, пайдаланушы ешқандай пішім белгілемесе ғана қолданылады. Қателер журналындағы қалыпты хабарлама мынадай:

```
[Fri Sep 09 10:42:29.902022 2011] [core:error] [pid 35708:tid 4328636416] [client
72.15.99.187] File does not exist: /usr/local/apache2/htdocs/favicon.ico
```

Журналдағы бірінші мәні – бұл хабарлама күні мен уақыты. Одан әрі хабарлама жолдаған модуль (бұл жағдайда — *core* — ядро) және хабарлама маңыздылығының деңгейі (бұл жағдайда — *error* — қате). Одан әрі хабарлама жолдаған процесс идентификаторы тұр (егер бұл өзекті болса — ағын идентификаторы). Содан кейін соның нәтижесінде хабарлама жолданған клиент мекенжайы. Хабарлама жолындағы соңғы элемент мәтіндік сипаттама, бұл жағдайда ол килентпен сұралған файл жоқ екенін көрсетіп тұр.

Журналдарда алуан түрлі хабарламалар пайда болуы мүмкін. Олардың басым бөлігі келтірілген мысалдағыға азды-көпті ұқсас болып келеді. Қателер журналында CGI скриптерінен алынған ретке келтіру қорытындылар болады. CGI-ден қателердің стандартты ағынына бағытталған кез-келген ақпарат тікелей осы журналға бағытталатын болады.

Ретке келтіру үшін *access_log*и *er- ror_log* баптауларына %L қосу ыңғайлы. Нәтижесінде, хабарлама идентификаторы екі журналға да жазылады және екі осы журнал жазбаларының сәйкестігін табу оңайырақ болады.

Сайтты тіркеу. Web-сервер қандай да бір тіркелусіз өз бетінше жұмыс істей алады. Алайда, оны ашу үшін серверге желілік қолжетімділікті алу және IP-мекенжай мен порт секілді оған қосылу параметрлерін білу қажет болады.

Бастапқы орнатулар бойынша стандарттарға сәйкес (егер, басқасы нақты белгіленбеген болса), http:// сұраныстары 80 портқа жіберіледі. Басқа порттарды қолданбаған дұрыс, себебі, бұл пайдаланушы үшін мекенжайды теруді қиындатады. Мысалы, *www. mysite. org* серверінде сайт орналастырып, пайдаланушы браузерде мынаны теруі керек:

```
http://www.mysite. org
```

Егер, Web-сервер стандартты емес портта (мысалы, 1080) орналасқан болса, онда браузердегі жазба портты нақтылаумен күрделене түседі:

```
http://www. mysite.org:1080
```

Жоғарыда сипатталғандай (1.8-бөлімшені қараңыз) белгілі бір сайт атына арналған HTTP-сұранысы нақты серверге келуі үшін сервердің DNS-атауы осы сервердің IP-мекен-жайында шешілуі қажет. Бұл жағдайда сайтты DNS-та тіркеу керек. Бұл 3.2-бөлімшеде сипатталған және мұнда қарастырылмайтын болады.

Оның Интернетте қолжетімді болуы үшін серверде «аппақ» IP-мекенжай болуы керек екеніне назар аударыңыз.Олай болмаған жағдайда,

TCP-пакеттерінің қайта адрестелуін бағыттауышта баптауға тура келеді. Серверді Интернетте ашу қажеттілігі болмаса, бұл талапты орындау міндетті емес. Интернетте қолжетімді күрделі желілердегі Web-серверлер әдетте демилитаризацияланғанаумақта болады.

Web-серверді құру кезінде интернет-провайдерге біршама көңіл аудару керек. Көптеген провайдерлер жеке тұлғаларға «аппақ» IP-мекенжайларын ұсынбайды. Егер, Web-серверді жеке тұлға үшін «көтеру» қажет болса, онда оған интернет-провайдерден тұрақты «аппақ» IP-мекенжайы бар сәйкес қызметті сұрау керек.

Жалға алынатын виртуалды немесе нақты серверлерді қолдану басқа әдіс болып табылады. Статикалық «аппақ» IP-мекенжайларды анықтау бұл жағдайда жалға берушіге жүктеледі.

Вирталды серверлердегі хостинг. Виртуалды сервер – виртуалды жеке серверді (VirtualPrivateServer— VPS) жалға беру қызметі қазір кеңінен таралған.

Виртуалды серверлер, әдетте, маңызды ірі жобалар үшін сатып алынатындықтан, олардың таңдауына өте мұқият қарау керек. Бұдан әрі VPS-хостингті таңдау кезінде есепке алу қажет негізгі факторлар жинақталған.

Хостингтік компанияның мәртебесі мен географиялық орналасуы. Таңдалған хостингтік компанияда заңды тұлға мәртебесі, сәйкес қызметтерді («телематикалық байланыс қызметі») ұсынуға арналған кеңсесі мен лицензиясының болуы маңызды.

Шұғыл сұрақтар туындаған жағдайда қоңырау шалуға арналған байланыс телефоны нөмірінің (тиісінше, 8-800 кодымен – Ресей қоңыраулары үшін тегін) болуына назар аударыңыз. Егер, хостердің сайтында тек электронды пошта немесе кері байланыс үлгісі ғана болып, телефон жоқ болса, онда бұл аталған компания өз жұмысының сапасына және ұзақтығына сенімді емес екенін немесе тіпті компания емес, жай ғана ақша таппақ болған студенттер екенін білдіреді.

Егер сізге қызықты болған хостер сізге VPS-те тегін сынақ мерзімін ұсынатын болса, онда оны пайдалану мүмкіндігінен қашпаңыз. Ұсынылған 5-30 күн ішінде сіздің сайтыңыздың онда қалай жұмыс істейтінін және осы виртуалды сервердің сіз үшін қолайлы ма екенін түсіне аласыз.

Серверлердің географиялық орналасуы. Егер, сайт орыс тілді пайдаланушыларға есептелген болса, онда VPS-серверді жалға алуды мүмкіндігінше Мәйскеуде, Санкт-Петербургте немесе Ресейдің басқа қаласында тапсырыс берген дұрыс. Көп жағдайда, сервер мақсатты пайдаланушыларға неғұрлым жақын орналасқан болса, мәліметтер жолдау жылдамдығы соғұрлым жылдам болады. Сервер орналасқан деректер-

орталығының үлкен географиялық қашықтығы жүктеу жылдамдығына кері әсер етуі мүмкін. Мысалы, Германиядағы серверлердің *(ping)* жауап беруінің орташа уақыты – 40-60 мс-ге тең, АҚШ-та – 80-100 мс болса, Ресей, Украина немесе Белоруссиядағы уақыт – 5-20 мс құрайды.

Екінші жағынан, еуропалық және американдық деректер орталығы әлдеқайда сенімдірек деген де пікір бар.

Басқару панелі. Егер, сіз қарапайымЕ виртуалды хостингтен VPS-серверге көшетін болсаңыз және Linux/FreeBSD басқару қабілетіңіз жоқ болса, онда сізге міндетті түрде жұмысты біршама жеңілдететін басқару панелі бар серверді таңдау керек. Көптеген компаниялар ISPmanager панелін, кей жағдайларда Plesk, DirectAdmin, cPanel панельдерін ұсынады. Кейбір компаниялар басқару панелін тегін ұсынса, кейбірі тариф ақысына қосымша төлемге ғана береді.

Сондай-ақ, басқару панелі виртуалды сервердің ресурстарын жұмсайтынын және оларды VPS-серверлерде 512 МБ-дан басталатын көлемдегі жедел жадымен орнату ұсынылады.

Техникалық қолдау. Барлық компаниялардың дерлік сайттарында техникалық қолдау қызметі тәулік бойы жұмыс жасайды деп жазылған. Шын мәнінде, өкінішке қарай, бәрі олай емес. Оны тексеру оңай: түнде сізді қызықтыратын компанияның сайтына кіріп, электрондық пошта арқылы немесе басқа тәсілмен қолдау қызметіне сауал жолдаңыз. Жауап беру жылдамдығынан басқа, қаншалықты сыпайы және сауатты жауап бергеніне назар аударыңыз.

Виртуалдандыру технологиясы. Вирталды серверге тапсырыс беру кезінде оның негізінде VPS-сервер жұмыс істейтін виртуалдандыру технологиясының таңдауына назар аудару керек. Көптеген компаниялар қалайтын OpenVZ ең кеңінен таралған жүйе болып табылады. Xen және KVM виртуалдандыру технологиялары едәуір аз танымал.

OpenVZ — бұл Linux ядросында негізделетін ОЖ деңгейіндегі виртуалдандыру технологиясын жүзеге асыру. OpenVZ бір ғана нақты серверде көптеген оқшауландырылған ОЖ көшірмелерін – виртуалды серверлерді іске қосуға мүмкіндік береді.

Алдын ала орнатылған бағдарламалық қамсыздандыру VPS сервері үшін бөлінген дисктік кеңістікті алады. OpenVZ виртуалды машиналарға немесе жартылай виртуалдандырғыш технологияларға қарағанда Linux ядросына негізделетіндіктен, «қонақ» жүйелер рөлінде тек Linux дистрибутивтері ғана бола алады. Алайда, OpenVZ-де ОЖ деңгейінде виртуалдандыру балама шешімдердегіге қарағанда өте жақсы өнімділік, масштабталу, орналасу тығыздығы, ресурстарды қарқынды басқару, сондай-ақ, басқару жеңілдігін береді. OpenVZ сайтына сәйкес,

виртуалдандыруға арналған үстеме шығындар өте аз және қарапайым Linux-жүйелермен салыстырғанда өнімділіктің төмендеуі небәрі 1-3%-ды құрайды. Кемшілігі біреу – ОЖ ядросы мен оның модульдерін ауыстыруға болмайды.

OpenVZ сайты Vir-tuozzo технологиясы үшін негізгі платформа болып табылады.

Xen – тегін болған 2009 жылдары үлкен танымдалдлыққа ие болған аппаратты виртуаландыру болып табылады. VDS сиртуалды серверлерінде түрлі ОЖ мен ядро ауыстыруы болуы мүмкін. Алдын ала орнатылған бағдарламалық қамсыздандыру VDS-ға бөлінген диск кеңістігін алады. Xen технологиясы виртуалды машиналар арасында сервердің жүйелік ресурстарының қатаң түрде бөлінуін жүзеге асырады және оверселлингтің (процессорлық уақыт пен жедел жадыда бар виртуалды машиналардан көп санының серверде орналастырылуы) болуына жол бермейді. Бұл басқа клиенттердің ресурсы тұтынуына тәуелсіз виртуалды сервер жұмысының сенімділігі, тұрақтылығы мен кепілдігін алуға мүмкіндік береді.

KVM (Kernel-basedVirtualMachine) — бұл x86 платформасындағы Linux ортасында виртуалдандыруды қамтамасыз ететін бағдарламалық шешім. KVM жұмысы үшін қажетті ядро құрауышы 2.6.20 нұсқадан бастап Linux-тің негізгі тармағына қосылған. KVM, сондай-ақ, ядро модулі ретінде FreeBSD-ге портталды. KVM өнімділігі аппараттық виртуалдандыру тәртібінде жұмыс істейтін Xen өнімділігімен салыстырылды және жүктемелердің белгілі бір түрлерінде KVM өте жақсы өнімділік көрсетті.

FreeBSD — ОЖ деңгейін виртуалдандыру. Барлық виртуалды орталар бірыңғай ядроны қолданады. VPS-серверлерде тек FreeBSD ОЖ ғана болуы мүмкін. Жоғары тығыздық пен VPS өз дискін аз тұтынуды артықшылықтардың бірі деп айтуға болады. Алдын ала орнатылған бағдарламалық қамсыздандыру виртуалды сервер үшін бөлінген диск кеңістігін алмайды.

Мониторинг. Web-сервер мониторингі кезінде мониторингтің көп деңгейін атап өтуге болады, сәйкесінше, түрлі бағдарламалық қамсыздандыру түрлі деңгейде сервер жұмысының мониторингімен айналыса алады. Nagios бастапқы ашық коды бар бағдарламалық қамсыздандыру негізіндегі мониторингті қарастырайық.

Web- сервер мониторингінің барлық ықтимал әдістерін ретімен атап көрсетейік.

Желілік тораптың қолжетімділігі. Егер, Web-сервер жұмыс істейтін ЭЕМ өзі желіде қолжетімді болмаса, сұраныстар Web-сервердің бағдарламалық қамсыздандыруына да жетпейді. Қолжетімділікті тексеруді

ICMP хаттамасы және *ping:* user@machine:~>ping -c 1 www. mysite. Org командасы арқылы жүргізу тиімдірек.

```
PING www.mysite.org (10.0.1.146) 56(84) bytes of data.
64 bytes from www. mysite. org (10.0.1.146): icmp seq=1 ttl=64 time=0.399 ms

---- www. mysite. org ping statistics ----------------------------
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.399/0.399/0.399/0.000 ms
```

Келітірлген мысалда сервер сәтті жауап бергені көрініп тұр. Сервермен байланыстың жоқтығы көптеген проблемаларды білдіруі мүмкін:

- ЭЕМ сөндірулі немесе қатып қалған;
- ЭЕМ-нің желіге қолжетімділігін қамтамасыз ететін желілік жабдық жұмыс істемей тұр;
- ЭЕМ-мен байланыстың нақты арналары жұмыс істемей тұр: сымның үзілуі, сым «ұясынан» шығып кетті;
- DNS-те ЭЕМ үшін жазба арналмаған;

```
user@machine:~> ping -c 1 www. mysite1. org ping: unknown
host www.mysite1.org
```

- ОЖ-де желіні қолдау сөндірулі және т.б.

TCP-сокеттің қолжетімділігі. Web-сервер сыртқы тораптардан қосылуды қабылдауы үшін ол тыңдайтын TCP-сокет қолжетімді болуы керек. Алдымен серверде сокет ашулы тұрғанын ашу маңызды. Ол үшін *netstat* командасын қолдануға болады:

```
user@machine:~/httpd> netstat -anpt | grep 8081 (Not all processes could be identified,
non-owned process info
will not be shown, you would have to be root to see it all.) tcp 0 0 127.0.0.1:8081
0.0.0.0:* LISTEN 701/httpd
```

Соңғы жол сокеттің тыңдалып жатқанын білдіреді. TCP-сокеттің қолжетімділігін басқа желілік тораптардан тексеру, әдетте, мақсатты сокетпен қосылуды ашуға және онымен хабарлама алмасуға мүмкіндік беретін *telnet* командасын қолданумен жүзеге асырылады:

```
user@machine:~/httpd/logs> telnet www. mysite.org 8081 Trying 127.0.0.1...
Connected to www.mysite.org.
Escape character is '^]'.
```

«Connectedto...» сөйлемінің болуы TCP бойынша қосулы сәтті өткенін білдіреді. Сессияны аяқтау үшін Crtl+] ( ]) басып, артынша *quit* командасын енгізу керек:

user@machine:~/httpd/logs> telnet www. mysite.org 8081 Trying 127.0.0.1...
Connected to www.mysite.org.
Escape character is ']'.
telnet>quitConnectionclosed.

TCP-сокетке қосылудың жоқтығы бағыттауыш қатесіне және брандмауерге байланысты болуы мүмкін.

HTTP-сұраныстарға жауап. Web-сервер жауаптарын, мысалы, *curl* командасының көмегімен тексеруге болады:

user@machine:~/httpd/logs> curl http://www. mysite. org:8081/
<html><body><h1>It works! (my site)</h1></body></html>

curl жауабын талдау кезінде тегсіз HTML-парақшасының ішіндегі қажет болуы мүмкін. Ол үшін html-ді қарапайым мәтінге түрлендіруге мүмкіндік беретін w3m консольдік Web-браузерді қолдануға болады:

user@machine:~/httpd/logs> w3m -T text/html -dump http://www.mysite.org:8081/
Itworks! (mysite)

Осылайша, қандай мәтін және қандай Web-тораптарда кездесуі керек екенін біліп, виртуалды тораптардың диагностикасын бекітіп қоюға болады.

***mod_status* мәртебесінің модулі.** Apache-де Web-сервер мәртебесінің мониторингін жүргізуге мүмкіндік беретін арнайы модуль — *mod_status* ұсынылған. Ол әкімшіге сервердің ағымдағы өнімділігін бағалауға мүмкіндік береді. Өнімділіктің көптеген параметрлері қарапайым оқу үшін HTML-парақша пішімінде құрылады. Сондай-ақ, мәтін түрінде де (HTML емес) ақпарат алу мүмкіндігі де бар.

Сервер мәртебесінің парақшасы келесі ақпаратты ұсынады:

- өңделетін сұраныстар саны;
- тұралап қалған ағындар (worker) саны;
- әрбір ағын мәртебесі, осы ағынмен орындалған сұраныстар саны және онымен өңделген байттар саны;
- қолжетімділік әрекетінің жалпы саны және өңделген байттар саны;
- серверді қосу/қайта қосу уақыты және сервердің әрекет ету уақыты (қосу/қайта қосу сәтінен бастап алынған уақыт);
- 1 с ішіндегі сұраныстардың орташа саны, бір секундтағы өңделген байттар саны және сұраныс үшін өңделген байттардың орташа саны;
- ағындар және барлық сервер бойынша орталық процессордың ресурстар тұтынуы;
- дәл қазіргі сәтте өңделіп жатқан сұраныстар.

Келітірілген қызметті қосу үшін *httpd. conf* файлына келесі жолдарды

жалғау қажет:

<Location /server-status>
SetHandler server-status Require host
localhost </Location>

Серверге жолданған сұраныс шамамен келесідей қорытынды береді:

user@machine:~/httpd/conf> w3m -T text/html -dump
http://www.myothersite.org:8081/server-status Apache Server Status for www.
myothersite. org (via
127.0. 0.1)

Server Version: Apache/2.4.7 (UNIX)
Server MPM: worker
Server Built: Jan 31 2014 11:49:57

Current Time: Tuesday, 29-Apr-2014 10:45:49 MSK
Restart Time: Tuesday, 29-Apr-2014 10:35:33 MSK
Parent Server Config. Generation: 1
Parent Server MPM Generation: 0
Server uptime: 10 minutes 15 seconds
Server load: 0.37 0.51 0.50
Total accesses: 12 - Total Traffic: 18 kB
CPU Usage: u0 s0 cu0 cs0
.0195 requests/sec - 29 B/second - 1536 B/request 1 requests currently being
processed, 99 idle workers
Scoreboard Key:
" " Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup, "C" Closing connection,
"L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

Srv PID Acc M CPU SS Req Conn Child Slot Client VHost Request
0- 0 13182 0/1/ 0.00 239 18 0.0
0.00 0.00
127.0. 0.1 www.mysite.org:8081
GET / HTTP/1.1
1

```
0-              0 13182          0/1/      _ 0.00       97          1          0.0
                0.00    0.00
localhost www. myothersite.org:8081 GET /server-status HTTP/1.1
                1
0-  0 13182   0/1/    _ 0.00     62          0          0.0        0.00       0.00
localhost www. myothersite. org:8081 GET /server- status?auto HTTP/1.1
                1
1-  0 13183   0/3/    _ 0.00     188         0          0.0        0.00       0.00
127.0.                                                  0.1 www. mysite.org:8081
                                                        NULL
                3
1-              0 13183          0/1/      _ 0.00       66          0          0.0
                0.00    0.00
localhost www. myothersite. org:8081 GET /server- status?auto HTTP/1.1 1
1-  0 13183   0/1/    _ 0.00     4           0          0.0        0.00       0.00
localhost www. myothersite.org:8081 GET /server-status HTTP/1.0
                1
2-  0 13186   0/1/    _ 0.00     182         7          0.0        0.00       0.00
localhost www.mysite.org:8081                           NULL
                1
2-              0 13186          0/1/      _ 0.00       64          1          0.0
                0.00    0.00
localhost www. myothersite.org:8081 GET /server-status HTTP/1.1
                1
2-              0 13186          0/0/      W 0.00       0           0          0.0
                0.00    0.00
3-          0.1 www. myothersite.org:8081 GET /server-status
4-          0 13881 0/1/ _ 0.00        8          0          0.0        0.00       0.00
localhost www. myothersite.org:8081GET /server- status?auto HTTP/1.0 1
3-                                  0 13881 0/1/ _ 0.00  72          1          0.0
                                    0.00        0.00
localhost www.myothersite. org:8081 GET /server- status?auto HTTP/1.1 1
```

Srv Child Server number - generation PID OS process ID
Acc Number of accesses this connection / this child / this slot
M Mode of operation
CPU CPU usage, number of seconds
SS Seconds since beginning of most recent request Req Milliseconds required to process most recent request

Conn Kilobytes transferred this connection Child Megabytes transferred this child Slot Total megabytes transferred this slot

Жиі жағдайда әлдеқайда интеллектуалды автоматты талдау жүргізуі керек басқа бағдарламалық қамсыздандыруға Web-сервер мәртебесін беру қажет. Мәртебені шығару кезінде артық ақпаратты болдырмас үшін сұраныс соңына *?auto* қосып жазып қоюға болады:

user@machine:~/httpd/conf> curl http://www. myothersite. org:8081/server-status?auto Total Accesses: 13 Total kBytes: 24 Uptime: 778 ReqPerSec: .0167095 BytesPerSec: 31.5887 BytesPerReq: 1890.46 BusyWorkers: 1 IdleWorkers: 99 Scoreboard: ___W _____

Бұл тұжырым бағдарламалық жасақтаманы талдауға әлдеқайда жеңіл.

Web-сервердің мәртебе парақшасы сервер ақауларын іздеу кезінде ыңғайлы болуы мүмкін, мысалы, Web-сервер орталық процессордың немесе ЖЖҚ-ның барлық ресурстарын тұтынған кезінде. Осы модуль көмегімен қандай сұраныс барлық жүйелік ресурстарды тұтынып жатқанын оңай анықтауға болады.

Ретке келтіруді тиімдірек ету үшін сервер конфигурациясына мәртебелік ақпаратты кеңейтетін жолдарды қосамыз:

ExtendedStatuson

Бұл директива бастапқы орнатулары бойынша сөндірілген, бірақ, оны кейбір Apache модульдарымен қосуға болады. Осылайша, ол мәртебелік парақшаны шығаруға әсерін бермеуі мүмкін.

1.10. Қауіпсіздік

Орнатылған Web-сервердің қауіпсіздігін қамтамасыз ету кезінде келесі негізгі әлсіздік көздерін ескеру қажет:

- Директорияға қолжетімділіктің қате баптаулары. Пайдаланушыға сервердің өте маңызды файлдарына қолжетімділік бере алады;
- Apache модульдерінің баптауларындағы қателер. Нәтижесінде сервердің маңызды файлдарына қолжетімділік ұсынылуы мүмкін немесе серверде қандай да бір ерікті кодтар орындалуы мүмкін. Мұндай қателер Apache ұсынған (*mod_rewrite.so* секілді) түрлі модульдар үшін ерекше болып келеді және олар мұнда қарастырылмайды;
- Сәйкестендіру және қолжетімділікті бақылау модульдерінің қате баптаулары;
- Web-серверде орнатылған Web-қосымшалардағы қателер. Бұл мәселенің шешімі мұнда қарастырылмайды, себебі, ол нақты қосымшалар үшін өзгеше.

Әрбір сайт үшін бапталатын тармақтарды жіті қарастырайық.

Директорияларға қолжетімділікті шектеу. Серверде сайт пайдаланушыларға қолжетімділікті ұсынуға болмайтын маңызды файлдар сақталуы мүмкін. Мысалы:

- Құпиясөздер хэші бар файлдар. Олар пайдаланушылардың құпиясөздерін анықтауға пайдаланылуы мүмкін;
- Сертификаттар мен қауіпсіздік кілттері. Олар басқа серверлер мен қызметтерге қолжетімділікті алу үшін, қол қойылған хабарландыруларды қолдан жасау, электрондық пошта бойынша қорғалған хат алмасуларды ашу, VPN арқылы ішкі желілерге қолжетімділікті ашу үшін пайдаланылуы мүмкін;

- Web-серверде сақталатын коммерциялық құпияға немесе жеке мәліметтерге жатқызылған құпия ақпарат. Бұл мәліметтерге пайдаланушылардың қолжетімділігі мүмкін болмау үшін директория қолжетімділігіне шектеу қою ұсынылған. Белгілі-бір директорияға (және оның шағын директорияларына) қолжетімділікті сипаттайтын *Directory* директивасын қарастырайық:

<Directory/usr/local/httpd/htdocs>
OptionsIndexesFollowSymLinks</Directory>

Директивалардың директорияларға қолдану әдісі. Директорияға жол не толық директорияға жол немесе UNIXShell секілді рәсімделген жол шаблоны болып келеді::

- [] — таңба диапазонын белгілеу үшін пайдалануға болады;
- ? — жеке таңбаларды белгілеу үшін;
- * — жолда таңбалардың ерікті бірізділігін белгілеу үшін.

Көрсетілген амалдардың ешбіреуі – таңба «/» - директория бөлгішін алмастырмайды. Осылайша,

<Directory /*/publichtml>

/home/user/public_html жолына сәйкес келмейді,бұл жағдайда осы жолға келесі директива сәйкес келетін болады:

<Directory/home/*/publichtml>

Тұрақты мәндер пайдаланылуы да мүмкін, мысалы:

<Directory~ "^A/www/[0-9]{3}">

Үш саннан есімі бар */www* директорияларына сәйкес келеді.

Егер, сервер директориясы <Directory> тегімен сипатталған көптеген директориялардың ішінде болса, осы тегтердегі директивалар көрсетілген тегте жол ұзындығының өсуі бойынша пайдаланылады. Мысал үшін келесі конфигурацияны алайық:

<Directory />
AllowOverride None

</Directory>

<Directory/home>
AllowOverride FileInfo
</Directory>

/home/web/dir/doc.html файлына қолжетімділігті анықтау үшін директивалар келесі тәртіпте қолданылады: *AllowOverride None* «/»-дан; *AllowOverride FileInfo «/home»*-нан.одан кейін */home/.htaccess, /home/web/. Htaccess* және */home/web/dir/.htaccess* файлдарындағы барлық директивалар қолданылады.

Тұрақты мәндермен көрсетілген директориялардағы директивалар <Directory> тегтері мен . *htaccess* файлдарындағы барлық директивалардан кейін қолданылады.

Бастапқы орнатулары бойынша Apache-де түпкі директорияға толық ашық қолжетімділік орнатылған. Бұл деген, егер, сайт директориясынан тыс жерде конфигурацияда директория пайдаланылатын болса, ол Web-серверде жария болатынын білдіреді. Сондықтан, бұл қолжетімділікке шек қою керек:

<Directory/>
Requirealldenied</Director
y>

Қолжетімділікиі шектеу директивалары. Директорияға қолжетімділікті басқаратын негізгі директива *Require* болып табылады.Оның мүмкін мәндерін қарастырайық:

- *Requireallgranted*— барлығына шартсыз қолжетімділік берілген;
- *Requirealldenied*— қолжетімділік шартсыз шектеулі;
- *Requireenvenv-var [env-var]* — егер, env-var жүйелік айнымалы орнатылған болса, қолжетімділік беріледі;
- *Requiremethodhttp-method [http-method]* — қолжетімділік белгілі-бір HTTP-әдісті (HTTP хаттамасы әдістер жинағын анықтайды: GET, PUT, DELETE, POST...) қолданған уақытта беріледі;
- *Requireexprexpression*— егер, *expression* мәнін анықтау нәтижесі ақиқат болса, қолжетімділік ұсынылады. Көптеген сәйкестендіру модульдері *Require* директивасының келесі үлгілерін пайдаланады:
- *Requreuseruserid [userid]* — қолжетімділік тек көрсетілген пайдаланушыға (пайдаланушылар тізіміне) берілген;
- *Requiregroupgroup-name [group-name]* — қолжетімділік тек көрсетілген топқа (топтар тізіміне) берілген;

- *Requirevalid-user* — қолжетімділік сәйкестендіруден өткен кез-келген пайдаланушыға берілген;
- *Requireipnetwork [network]* — қолжетімділік тек белгіленген желілерден қосылған пайдаланушылар үшін ұсынылған.

Көптеген директивалар. IP-мекенжайы бойынша қолжетімділікті шектеу мысалында ережелерді қолдану тәртібін қарастырайық. Желіде түрлі қолжетімділік сегменттері бөлінетінге байланысты бұл шектеу жиі пайдаланылады.

mysite. org қолжетімділігін келесі әдіспен баптаймыз:

```
<Directory "/home/user/httpd/htdocs/mysite">
        Require all denied Require ip
127.0.0.1 </Directory>
```

Бұл ретте, серверге сұраныс жергілікті хосттан сәтті орындалады:

```
user@machine:~/httpd/conf> curl http://www.mysite. org:8081/
<html><body><h1>It works! (my site)</h1></body></html>
```

Require директивасының бірізділігін өзгертеміз*:*

```
<Directory "/home/user/httpd/htdocs/mysite">
        Require ip 127.0.0.1 Require all
denied </Directory>
```

Бұл ретте, торапқа қолжетімділік жергілікті тораптан, бірақ, басқа тораптан емес, сәтті ұсынылған болады. Дегенмен, *Requireip* жазбасын жойған уақытта қолжетімділікке шектеу қойылады.

```
<Directory "/home/user/httpd/htdocs/mysite">
        Require all denied
</Directory>
```

Қолжетімділікті тексеру шектеуді көрсетеді:

```
user@machine:~/httpd/conf> curl http://www. mysite. org:8081/
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access / on this server.</p>
</body></html>
```

Жоғарыдағы мысалдан көріп отырғанымыздай, қол жеткізуді бақылау (авторизациялау) сәтті жұмыс істейді, бірақ, *Require* директивалар талаптарын жариялау тәртібіне байланысты емес. Бұл, бастапқы орнатулар

бойынша бір директива ішіндегі барлық директивалар логикалық «НЕМЕСЕ»-мен байланысады. Басқаша айтқанда, егер, бір ғана *Require* директивасы сәтті орындалса, қолжетімділік беріледі.

Қолжетімділік директивалары үшін логикалық оператордың бірігуіне айқын тапсырма мүмкіндігі бар: *RequreAll* және *RequireAny* директивалары.олар қолжетімділік директивасы келтірілген тегтер түрінде жарияланады, олардың нәтижелері бірігеді, сәйкесінше, логикалық «ЖӘНЕ» және «НЕМЕСЕ» бойынша:

```
<Directory "/home/user/httpd/htdocs/mysite"><RequireAll>
            Require all denied Require ip
      127.0.0.1 </RequireAll>
</Directory>
```

Requirealldenied қолжетімділік шарты ешқашан орындалмайтындықтан, келтірілген шарт ешқашан жүзеге аспайтыны анық. Серверге сұраныс кезінде күтілген нәтижені аламыз:

```
user@machine:~/httpd/conf>curlhttp://www. mysite. org:8081/
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access / on this server.</p>
</body></html>
```

RequireAny директивалары да осы секілді:

```
<Directory "/home/user/httpd/htdocs/mysite"><RequireAny>
            Require all denied Require ip
            127.0.0.1
      </RequireAny>
</Directory>
```

Қолжетімділікті анықтау тек *Requireip-ке* тәуелді болғандықтан, *Requirealldenied* мәні жоғалтқаны айқын.

Пайдаланушылар мен топтар. Көптеген сайттар пайдаланушылар мен топтар негізінде қолжетімділікті шектеуді қолдайды. Apache серверінде осындай конфигурацияны қарастырайық.

Apache –дегі сәйкестендіру жүйесіне мыналар кіреді:

- Сәйкестендіру провайдері (authenicationprovider) — пайдаланушының куәлігіне, мысалы, оның құпиясөзін тексеру, жауап беретін модуль;
- Сәйкестендірудің бапталған провайдерлерін пайдаланатын қолжетімділік директивалары.

Қарапайым аутентификация провайдерін қарастырайық - Apache арқылы қолжетімді файлда пайдаланушы құпиясөздерін сақтау. Оған

mod_authn_file модулі жауапты.Бұл провайдер өте жеңіл бапталады – бір ғана жолмен:

AuthUserFileconf/user-pass-file

File user-pass-файлының жолы серверді орнатудың түбірлік каталогына қатысты (1.6-бөлімшеден *ServerRoot* директивасын қараңыз). Файлдың әрбір жолында қос нүкте арқылы бөлінген пайдаланушы аты және шифрланған құпиясөз бар. Бірдей пайдаланушы бірнеше рет айтылса, провайдер тек құпиясөзбен бірінші жолды пайдаланады. Сайт арқылы пайдаланушыларға қол жетімді каталогта құпия сөзді сақтамаңыз, өйткені бұл барлық құпиясөздерді жарамсыз ету үшін пайдаланылуы мүмкін.

Құпиясөз файлын құру үшін Apache құрамына кіретін *htpasswd* утилитасын пайдалануға болады. Аталған файлды құрастырайық:

user@machine:~/httpd/htdocs/mysite> ../../bin/htpass- wd -c user-pass-file user1 New password:
Re-type new password:
Adding password for user user1
user@machine:~/httpd/htdocs/mysite> ../../bin/ htpasswd user-pass-file
user2 New password:
Re-type new password:
Adding password for user user2

С кілті жаңа құпиясөздер файлын жасау үшін пайдаланылады. Файлдың пішімінің бұрын сипатталған сипаттамасына сәйкес файлдың дұрыс жасалуына көз жеткізіңіз:

user@machine:~/httpd/htdocs/mysite> cat user-pass-file
user1:$apr1$tgJwNPFk$HpyBLDAKHeVKdFuVJTR6g1
user2:$apr1$m08.Ni0P$VwE21heYthqgm3cvn602X.

Осы файлды қолдана отырып, конфигурация файлын сәйкестендіруге қосамыз:

<AuthnProviderAlias file file1>
AuthUserFile conf/user-pass-file </AuthnProviderAlias>

<Directory "/home/user/httpd/htdocs/mysite"> AuthBasicProvider filel AuthType Basic
AuthName "Protected Area"
Require valid-user #Require ip
127.0.0.1 </Directory>

Консольден серверге қосылу 401 қателігін көрсетеді:

user@machine:~/httpd/conf> curl mysite.org:8081 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head>

<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.
</body></html>

Бұл қате сәйкестендіру қажеттігін көрсетеді. Мұндай қате шығарылған жағдайда браузер пайдаланушыға сервердегі есептік мәліметтерді енгізуге арналған терезені шағырады. Осы сайтты дұрыс және қате құпиясөз көрсету арқылы ашып көрейік:

```
user@machine:~/httpd/conf> curl --basic -u user1:111 mysite.org:8081
<html><body><h1>It works! (my site)</h1></body></html>
user@machine:~/httpd/conf> curl --basic -u user1:1112 mysite.org:8081
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.</p>
</body></html>
```

Көрсетілгендей, сервер дұрыс құпиясөзді қабылдайды да, керісінше, қате құпиясөзді қабыл алмайды. Енді екі пайдаланушы үшін қолжетімділік құқығын өзгертіп көрейік. Ол үшін, *userl* пайдаланушысына ғана қолжетімді *secret* директориясын сайтқа қосайық*:*

```
<Directory "/home/user/httpd/htdocs/mysite/secret"> AuthBasicProvider filel AuthType
    Basic
    AuthName "Very protected Area"
    Require user userl </Directory>
```

Осы директорияда директорияны сәйкестендіретін *index.html* файлын қосайық:

```
<html><body><h1>It works! (my site secret area)</h1></ body></html>
```

Протестируемдоступ:

```
user@machine:~/httpd/conf> curl --basic -u user1:111 http://mysite.org:8081/secret/
<html><body><h1>It works! (my site secret area)</h1></ body></html>
user@machine:~/httpd/conf> curl --basic -u user2:222 http://mysite.org:8081/secret/
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML
```

```
2.0//EN"><html><head><title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you are authorized to access the document
requested. Either you supplied the wrong credentials (e.g., bad password), or your
browser doesn't understand how to supply the credentials required.</p>
</body></html>
```

Осы сәтсіз әрекеттерден кейін mysite-error.log сайтының журналында келесідей жазбаларды көруге болады:

```
[Fri Mar 07 12:19:43.898904 2014] [auth_basic:error]
[pid 9762:tid 139804326151936] [client 127.0.0.1:39840] AH01617: user user1:
authentication failure for "/": Password Mismatch
[Fri Mar 07 12:24:56.761884 2014] [authz_ core:error] [pid 10723:tid
139804334544640] [client 127.0.0.1:39899] AH01631: user user2: authorization failure
for "/secret/":
```

Тұжырымдамадағы айырмашылықтарға назар аударыңыз. Қате құпиясөзді енгізген кезде құпиясөз сәйкес келмеді деп жазылған: аутентификация сатысының, яғни құпиясөзді тексеру қатесі.

Екінші жолда авторландыру қателігі орын алды деп жазылған, яғни, құпиясөз сәйкес келді, бірақ, сервер баптаулары пайдаланушыға директорияға жүгінуге рұқсат етпейді */secret/*.

Пайдаланушылар мен топтар қолжетімділігін бақылау. Apache журналының файлына қандай пайдаланушы белгілі бір ресурсты сұрағаны туралы ақпарат жазылады. Қолжетімділікті қатаң шектеу қажет болған жағдайда пайдаланушыларға ұсынылатын ресурстарды бақылап отыру үшін бұл журналдарды тұрақты түрде қарап отыру керек.

Автоматты индекстеуді өшіру. Директория индексі — бұл қандай да бір директория (нақты бір файлдыкі емес) клиентінің сұранысына жауап ретінде сервер жолдайтын парақша. Ол екі негізгі көздерден келуі мүмкін:

1) Пайдаланушымен жазылған файл (әдетте — *index. html). DirectoryIndex* директивасы осы файл атауын көрсетеді. Бұл әрекет *mod_dir* модулімен бақыланады;
2) Сервермен өндірілген директория файлдарының тізімі. Кейбір директивалар осы тізім пішімін баптайды. *AddIcon, AddIconByEncoding*и *AddIconByType* директивалары файлдарға арналған сүйемелдеу белгішелерімен басқарады. Бұл әрекет *mod_autoindex* модулімен орындалады.

Бұл екі нұсқа да мүлде тәуелсіз болып табылады, сондықтан, пайдаланушы олардың біреуін таңдай алады.

Директориялар индексін автоматты түрлендіру *Options* директивасымен қосылады:

Options +Indexes

Пайдаланушыға директориядағы барлық файлдардың тізімін ұсыну қауіпті болуы мүмкін, сондықтан автоматты индекстеуді өшіру ұсынылады. Егер, индекстеу бұған дейін қосылған болса, оны келесідей үлгіде сөндіруге болады:

Options -Indexes

Бұл кезде Apache конфигурация файлының тегтері ішіндегі директивалардың көріну аймағын да назарға алу керек.

Ашық кілтпен шифрлеу, сертификаттар. Бүгінгі таңда криптографияның кең таралған үлгілерінің бірі – ашық кілттердегі криптография болып табылады. Ашық кілттердегі криптография ашық (public) және құпия (secret) кілттерді пайдаланады. Жүйе ашық кілтті қолданумен шифрлеуді орындайды. Мұндай ақпарат тек құпия кілтті қолданумен ғана құпия шифры ашылады.

Ашық кілттердегі криптографияны әдеттегі қолдану - SSL мен TLS хаттамалары бойынша қосылуларды қолданумен қосымшалар трафигін шифрлеу, мысалы, SSL үстіне HTTP хаттамасы үшін, HTTPS ұсыну үшін Apache баптаулары. Бұл өз бетінше шифрлеуі жоқ хаттамасы бар трафикті шифрлеуді қолдануға мүмкіндік береді.

Сертификат — бұл ашық кілтті және сервер мен ол үшін жауапты мекеме туралы басқа да ақпаратты тарату үшін қолданылатын әдіс. Сертификаттарда сертификаттау орталығымен немесе CA әзірлеген сандық қолтаңба болуы мүмкін. CA – бұл сертификаттағы ақпараттың дұрыс екенін растайтын үшінші тарап.

Сертификаттар түрлері. Ашық кілттердегі криптографияны пайдаланып, қауіпсіз серверді орнату үшін, көп жағдайда, сертификатқа (соның ішінде ашық кілті бар) сұраныс, компания сәйкестігіне растау және сертификаттау орталығына төлем жіберіледі. Орталық сертификатқа пен сәйкестік сұранысын тексереді, содан кейін жауап ретінде серверге арналған сертификат жібереді.

Баламасы ретінде өздігінен қол қойған сертифкатты қолдануға болады.

Назар аударыңыз, өздігінен қол қойған сертификат өндірістік орталардың басым бөлігінде қолданыла алмайды.

HTTPS бар мысалды жалғастыра отырып, CA қол қойған сертификат өздігінен қол қойған сертифкаттан өзгеше екі маңызды қасиетті ұсынады.

1. Браузерлер (әдетте) мұндай сертифкатты автоматты түрде таниды және пайдаланушыны ескертусіз, қорғалған қосылуларды орнатуға мүмкіндік береді.
2. CA қол қойылған сертификатты шығарған кезде ол браузерге интернет парақшаларын ұсынатын ұйымның сәйкестігін кепілдендіреді.

Көптеген интернет-браузерлер мен SSL-ді қолдайтын компьютерлерде

куәліктері олардың сертификаттарын автоматты түрде қабылдайтын сертификаттау органдарының тізімі болады. Егер браузер куәландырушы орталығы осы тізімге енгізілмеген сертификатты кездестірсе, ол пайдаланушыны растауды немесе қосылуға тыйым салуды сұрайды. Бұл жағдайда, өздігінен қол қойған сертификат қолданылатын кезде басқа қосымшалар қате туралы хабарлама шығаруы мүмкін.

CA-дан сертификат алу процесі айтарлықтай қарапайым.

1. Ашық және құпия кілттерден жұп әзірленеді.
2. Ашық кілт негізінде сертификатқа сұраныс құрылады. Сертификатқа арналған сұраныс құрамында мақсатты сервер мен оны басқару компаниясы туралы ақпарат болады.
3. Мекеме сәйкестігін растайтын құжаттармен (мысалы, онда мақсатты сервер қарайтын мекеме атауы болады) бірге сертифкатқа сұраныс жолданады.
4. Орталық сұраныс жолдап отырған мекеменің шынайы екеніне көз жеткізген соң, тапсырыс берушіге сандық сертификат жолдайды.
5. Сертификат қорғалған мақсатты серверге орнатылады және оны қолдануға арналған сәйкес қосымшалар күйге келтіріледі.

Сертификатқа қол қоюға арналған сұранысты құру. CA-дан сертификат алу қажет болсын немесе өздігінен қол қойған сертификат жеткілікті болсын, бәрібір ең бірінші қадам – кілт жасау болып табылады. Егер, сертификат Apache, Postfix, Dovecot секілді жүйелік сервистермен қолданылатын болса, құпиясөзі жоқ кілт құру дұрыс болады. Құпиясөздің болмауы сервиске минималды қолдан араласумен бастай алады, әдетте, бұл сервисті іске қосудың ең қолайлы нұсқасы.

Бұл бөлімде құпиясөзі бар және жоқ кілтті қалай жасау керектігі көрсетіледі. Құпиясөзсіз кілт одан соң түрлі жүйелік қызметтер үшін қолдануға болатын сертификатты жасау үшін пайдаланылады.

Қорғалған Web-серверді кодты сөйлемсіз іске қосу осы серверді әр іске қосу кезінде әкімшіге оны енгізіп отыру қажет болмайтындығымен қолайлы. Алайда, бұл қауіпсіз, сондықтан, кілттің беделін түсіру бұл сервердің беделін түсіру болып табылады.

Сертификатқа қол қоюға арналған сұраныс кілттерін құру үшін (CSR) терминалдағы келесі команданы орындау қажет:

```
openssl genrsa -des3 -out server. key 2048

Generating RSA private key, 2048 bit long modulus e is 65537 (0x10001)
Enter pass phrase for server. key:
```

Пайда болған шақыруда пайдаланушыға кілтке арналған құпиясөзді енгізу қажет. Өте жақсы қауіпсіздік үшін кемінде сегіз таңба қолдану ұсынылады. *des*3 – қолдану кезіндегі минималды ұзындық – 4 таңба. Сөйлемде сандар және (немесе) тыныс белгілері болуы керек және

сөздіктегі сөз болмауы керек.

Одан әрі пайдаланушыға тексеру (қате теруден қорғаныс) үшін құпиясөзді енгізуді қайталау ұсынылады. Дұрыс енгізілген жағдайда сервер кілті құрылады және *server. key* файлына жазылады.

Енді кодты сөйлемі жоқ қауіпті кілт құрып, кілттердің атауын өзгертейік:

```
openssl rsa -in server. key -out server. key.insecure mv server. key server. key.
secure mv server. key.insecure server. key
```

Қауіпті кілт енді *server key* деп аталады және оны кодты сөйлемсіз CSR құру үшін қолдануға болады.

CSR құру үшін терминалдағы келесі команданы орындау қажет:

```
openssl req -new -key server. key -out server. csr
```

Бұл жағдайда кодты сөйлем сұралады (құпиясөзі бар кілт қолданылған жағдайда). Егер, дұрыс сөйлем енгізілген болса, компания атауын, сайт атауын, e-mail және т.б. енгізу қажет. Осы ақпараттың барлығы енгізілген соң CSR сұраныс құрылады және *server. csr* файлға сақталады.

CSR құрылған файлын өңдеу үшін сертификаттау орталығына жолдауға болады. CA орталығы бұл файлды сертификат шығару үшін қолданады. Алайда, CA-мен жұмыс жасау мүмкін болмаған жағдайда, дәл сол CSR көмегімен өздігінен қол қойған сертификатты құруға болады.

Өздігінен қол қойған сертифкат құру. Өздігінен қол қойған сертификат құру терминалдағы келесі командамен жүзеге асырылады:

```
openssl x509 -req -days 365 -in server. csr-signkey server. key -out server. crt
```

Бұл команда пайдаланушыдан кодты сөйлем енгізуін сұрайды. Содан кейін бірден жаңа сертифкат құрылады және *server. crt* файлға сақталады.

Егер, қорғалған мақсатты сервер өндірісте қолданылатын болса, сертификаттау орталығымен қол қойылған сертифкат қажет болады. Бұл жағдайда өздігінен қол қойған сертификаттарды қолданбау ұсынылады.

Сертификатты орнату. Алынған файлдар арасында келесі команданы іске қосу арқылы *server. key* кілті мен *server. crt* сертификаты (немесе CA-мен берілген сертификат файлы) кілтінің файлдарын орнатуға болады:

```
sudo cp server.crt /etc/ssl/certs sudo cp
server.key/etc/ssl/private
```

Кілт пен сертификаттың осы файлдарын орындауға арналған ашық кілттердегі криптографияны қолдану мүмкіндігімен кез-келген қосымшаны күйге келтіруге болады. Мысалы, Apache HTTPS ұсына алады,

ал Dovecot болса IMAPS пен POP3S ұсынады және т.б.

Сертификаттау орталығы. Егер желі сервистері өздігінен қол қойылған сертификаттардан басқа көпті талап етсе, өзіңіздің жеке ішкі сертификаттау орталығыңызды (CA) орнату бойынша қосымша күшейту пайдалы болуы мүмкін. Өзіңіздің орталығыңыз қол қойған сертификаттарды пайдалану әртүрлі қызметтерге дәл сол CA-мен берілген сертификаттарды пайдаланатын басқа қызметтерге жай ғана сену үшін қолдануға мүмкіндік береді.

CA сертификаты мен қажетті файлдарды сақтауға арналған каталогтар құрайық:

```
sudo mkdir /etc/ssl/CA sudo mkdir
/etc/ssl/newcerts
```

Сертификаттау орталығы өз жұмысының мақсатында бірнеше қосымша файлды талап етеді: бірінші – CA қолданған соңғы сериялық нөмірді сақтау үшін; екіншісі – шығарылған сертификаттардың жазбасы үшін:

```
sudo sh -c "echo '01' > /etc/ssl/CA/serial" sudo touch
/etc/ssl/CA/index.txt
```

Үшінші файл — CA баптауларының файлы. Ол қатаң түрде міндетті болмаса да, ол көптеген сертификаттарды шығару үшін өте қолайлы. *[CA_default]* секциясын өзгерту арқылы */etc/ssl/openssl.cnf* түзетуге болады:

```
dir = /etc/ssl/ # Where every
thing is kept
database = $dir/CA/index. txt # database index
file.
certificate = $dir/certs/cacert.pem # The CA certificate
serial = $dir/CA/serial # The current
serial number
private key = $dir/private/cakey. pem# The private key
```

Одан әрі өздігінен қол қойған сертификат құрылады:

```
openssl req -new -x509 -extensions v3 ca -keyout cakey. pem -out cacert. pem -days
3650
```

Пайдаланушыға сертифкат мәліметтері бойынша сұрақтар қойылады.

Одан әрі түпкілікті сертифкат пен кілт орнату қажет:

```
sudo mv cakey.pem/etc/ssl/private/ sudo mv
cacert.pem/etc/ssl/certs/
```

Енді, сертификаттар шығаруға кіріссе болады. Ең алдымен қажет болатыны – бұл сертификатқа сұраныс (CSR). Оны құру мәселелері бұған

дейін айтылды. CSR алған соң, жеке куәландырушы орталық сертификатының көмегімен оған қол қоюға болады:

```
sudo openssl ca -in server. csr-config /etc/ssl/openssl. cnf
```

CA кілтіне арналған құпиясөзді енгізгеннен кейін сертификатқа қол қоюға арналған және тағы біреуі жаңа сертификатты сақтауға сұралады. Бұдан соң алдыңғы қорытындыдағыдай мазмұны бар */etc/ssl/newcerts/01. pem* файлы пайда болуы керек. *BEGINCERTIFICATE* ---------- пен
---- *ENDCERTIFICATE*------- жолдары арасында осы файлда тұрғанның барлығын ол орнатылуы керек сервердің желелік атауы бар файлға сақталуы керек. Мысалы, *mail, example, com. crt* — айтарлықтай жақсы сипаттама атау. Мұндай файлдың әдеттегі құрамы мынадай түрде болады:

```
-------- BEGINCERTIFICATE ----------
MIIFyzCCA7mgAwIBAgIBHzANBgkqhkiG9w0BAQUFADCBpzELMAkGA
1UEBhMCUlUx
FTATBgNVBAgMDFJ5YXphbiBzdGF0ZTEPMA0GA1UEBwwGUnlhemFuM
RcwFQYDVQQK

66SGXS5j1reKRnHbOFYtqde/OERBfPvPn3LjKp3vUaLFINWP1DEOj
6iroeEiIKg=
-------- ENDCERTIFICATE ----------
```

Келесі сенртификаттардың атауы *02, pem, 03, pem* және т.б. болады.

Соңғы кезеңде, сертификат арнайы соған шығарылған компьютерге аталған сертификатты көшіріп, оны қолдану үшін сәйкес қосымшаларды баптау қажет. Сертификаттарды орнатуға арналған бастапқы орын – */etc/ssl/certs* каталогы. Бұл көптеген қызметтерге дәл сол бір сертификатты файлға қолжетімділік құқықтарын күрделендірмей пайдалануға мүмкіндік береді.

CA сертификаттарын қолдану үшін бапталуы мүмкін қосымшалар үшін */etc/ssl/certs/cacert, pem* файлын әрбір серверде */etc/ssl/certs/* каталогына көшіруге болады.

Apache-де сертификаттарды баптау. Apache конфигурациялық файлында SSL жұмысын қосу қажет:

```
SSLEngineon
```

SSLv2 ескірген хаттамасын қолдануға тыйым салу үшін келесі жолды қосу ұсынылады:

```
SSLProtocolall -SSLv2
```

Сертификаттар сервер сертификаты мен оның жеке кілтін көрсететін *SSLCertificateFile*и *SSLCertificateKeyFile* директиваларымен күйге келтіріледі:

```
# Сервердің көпшілік сертификаты
SSLCertificateFile /etc/ssl/certs/server.pem
# Сервердің жеке кілті
SSLCertificateKeyFile /etc/ssl/private/server.key
```

Apache-ні қайта жүктеген соң SSL механизмі іске қосылады. SSL қосу Apache-дегі арнайы портты ашпайтынына назар аударыңыз. SSL-дің көріну аумағы виртуалды хосттармен шектеледі. Осылайша, HTTP бойынша да, HTTPS бойынша да қолжетімді болуы үшін олардың бірінде SSL механизмін баптау қажет порттар бойынша екі ұқсас виртуалды хост құру қажет.

1.11. ҮДЕМЕЛІ WEB-ПАРАҚШАЛАР

Бұған дейін статикалық деп аталатын сайттардың мысалдары қарастырылған болатын. Ол – HTML және басқа да пішімде алдын ала құрылған файлдар жинағынан тұратын сайттар. Интернет-баламасын, фирма визиткасын әзірлеу оның міндеті болып табылатын көптеген сайттар үшін осындай технологиялар қалыпты болып табылады. Алайда, экономиканы ақпараттандырудың дамуымен көптеген сайттар пайдаланушыға уақыт ішінде өзгеретін мәліметтер ұсынады. Алуан түрлі интернет-дүкендер осының жарқын мысалы болып табылады. Теориялық тұрғыда сайтта жариялау үшін дүкеннің прайс-парағын қолмен жасауға болады. Алайда, баға немесе тауар сипатының немесе тауарлар тізімінің әрбір өзгеруі сайтты түзету қажеттілігіне алып келеді. Сайт орналасқан серверге қолжетімділік құқығы әдетте шектеулі болғандықтан, мұндай әрбір операция үшін сайтты әкімшілендіру үшін жауапты қызметкерді тарту керек болар еді.

Сервер жағындағы ендірмелер. Заманауи инернет-индустрияда басқа әдіс қолға алынған – бұл үдемелі сайттар құру. Пайдаланушылық сұранысты сервердің өңдеуі процесінде HTML-кодын «жылдам» құру ең қарапайым әрі жеңіл нұсқа болып табылады.

Жүйе пайдаланушылары туралы ақпарат ұсынатын қызметті қарастырайық. Соңғы пайдаланушы мынаған ұқсас HTML-код алуы керек:

```
<html>
    <table>
        <tr>
            <th>user ID</th><th>Full
        name</th><th>E-
```

```
    mail</th><th>groups</th></tr>
    <tr>
    <td>pbaranchikov</td>
            <td>Pavel Baranchikov</td>
            <td>pbaranchikov@cryptoanalytics.org</td><td>dev</td>
        </tr>
        <tr>
            <td>ipetrov</td>
            <td>Ivan Petrov </td>
            <td>ipetrov@cryptoanalytics. org</td><td>administrators</td>
        </tr>
        <tr>
            <td>vsidorov</td>
            <td>Vasily Sidorov</td>
            <td>vsidorov@cryptoanalytics. org</td><td>dev</td>
        </tr>
    </table>
</html>
```

Кодтан бірден үш элементті бөлуге болатыны көрініп тұр:

1) *тақырыбы:*

```
<html>
    <table>
        <tr>
            <th>user ID</th>
            <th>Full name</th>
            <th>E-mail</th>
            <th>groups</th>
        </tr>
```

2) *пайдаланушыны сипаттау үлгісі:*

```
        <tr>
            <td>ipetrov</td>
            <td>Ivan Petrov </td>
            <td>ipetrov@cryptoanalytics. org</td><td>administrators</td>
        </tr>
```

3) *соңы:*

```
    </table>
</html>
```

Пайдаланушы сипаттамасы пайдаланушыға сәйкес келетін жолдарды өзгертумен көп мәрте қайталанады. Тиісінше, сәйкес жолдарды алмастырумен циклдік қайталау көмегімен барлық қажетті кодты

түрлендіруге болады. Мұндай әдіс кеңінен таралған, бұл, клиентке (браузерге) жәй ғана HTML берілетіні және кез-келген браузер оны дұрыс аша алатынымен байланысты.

HTML түрлендіру CGI, PHP, JSP секілді бағдарламалау тілдері мен технологиялармен пайдаланылады.

CGI. CGI – сыртқы бағдарламаның Web-**сервермен байланыстыру үшін қолданылатын интерфейс стандарты – варқылы жүзеге асыруды қарастырайық.** Web-сервермен бірге мұндай интерфейспен жұмыс істейтін бағдарламаны шлюз деп атайды, бірақ, көбіне оны «скрипт» (сценарий) немесе «CGI- бағдарлама» деп те атайды.

Интерфейс стандартты енгізу-шығару құрылғыларымен жұмыс атқара алатын кез-келген бағдарламалау тілін қолдануға мүмкін болатындай жасалған. Мұндай мүмкіндіктермен БЖ командалық интерпретаторларға арналған скрипттерде де бар, сондықтан, қарапайым жағдайларда командалық скрипттер де қолданылуы мүмкін.

Әдетте, барлық скрипттарды сервердің *cgi* (немесе *cgi-bin)* каталогына орналастырады, бірақ ол міндетті емес: скрипт кез-келген жерде орналаса алады, бірақ, сонымен бірге, көптеген Web-серверлер арнайы баптауды талап етеді. Мысалы, Apache Web-серверінде мұндай баптау *httpd. Conf* баптаудың жалпы файлы көмегімен немесе осы скрипт орналасқан каталогта . *htaccess* файлы көмегімен жүзеге асырыла алады.

CGI динамикалық Web-парақшаларды құрастырудың ең кең тараған құралы болып табылады. CGI жұмысын іске қосу үшін Apache-ге CGI*(mod_cgi)* модулін жүктеу қажет.

ScriptAlias директивасы CGI-бағдарламалар орналасқан нақты директорияларды белгілеу үшін пайдаланылады.

Apache бұл директорияда файлдарды CGI-бағдарламалар секілді қабылдайды және оларға пайдаланушы тапсырыс берген жағдайда оны орындауға тырысады.

CGI-директорияны конфигурация файлына қосамыз:

```
ScriptAlias /cgi-bin/ "/home/user/httpd/cgi-bin/"
```

Бастапқы баптаулар бойынша бұл директива <IfModulealias_module> тегі ішінде қосылған. Apache орнатулары құрамына технологияның мүмкіндіктерін зерттеуге мүмкін болатын CGI-бағдарламаларының мысалдары енгізілген. Олардың негізінде серверде ағымдағы уақытты қайта келтіретін кіші бағдарламаны Bash-қа құрастырып көреміз:

```
#!/bin/sh

echo -n "Current server time is " date "+%F %T"
```

Бағдарламаны */home/user/cgi-bin/getdate* сақтаймыз және оның орындалуына рұқсат береміз:

```
user@machine:~/httpd/cgi-bin> chmod ug+x getdate user@machine:~/httpd/cgi-bin>
./getdate Current server time is 2014-03-12 11:26:59
```

CGI-бағдарламалар міндетті түрде орындалу қажет, дәл осы мақсат үшін *chmod* командасы пайдаланылды. Листингте көрсетілгендей, бағдарлама күтілгендей сервердегі ағымдағы уақытты қайта келтіріп отырды. Енді, Apache-ні іске қосамыз да осы бағдарламаға браузер арқылы сұраныс жібереміз:

```
user@machine:~/httpd/cgi-bin> curl http://mysite.
org:8081/cgi-bin/getdate
#!/bin/sh

echo -n "Current server time is " date "+%F %T"
```

Бұл жауапқа қарағанда Apache сервері бағдарламаны CGI-бағдарлама ретінде қабылдаған жоқ, керісінше, оның құрамын қарапайым мәтіндік файл ретінде көрсетті. Бұл CGI-бағдарламарды өңдеуге арналған Apache модулі жүктелмегенмен байланысты. Конфигурация жолын өзгертіп, оны іске қосамыз:

```
LoadModulecgidmodulemodules/modcgid. so
```

Apache-нің жаңа нұсқаларында *mod_cgi* модулі мүлде компиляцияланбайды. Оның орнына конфигурациялық файлда аталған *mod_cgid* модулі жеткізіледі. Көптеген UNIX ОЖ-де көптеген ағындардан тұратын процестен еншілес процесс құру шығынды әрекет болып табылады, себебі, жаңа процестің ағындары дәл сол бас процестікіндей болады. Сондықтан, *mod_cgid* модулін әзірлейік, ол CGI-бағдарламаларын өңдейтін еншілес процестерді құруға жауап беретін жекелеген демон-процесс құрады. Apache негізгі сервері бұл демонмен UNIX-сокеттер (сокеты Беркли) арқылы байланысады.

Құрылған CGI-бағдарламасын іске қосуға тырысайық:

```
user@machine:~/tmp/httpd-install/conf> curl http:// mysite.org:8081/cgi-bin/getdate
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head>
<title>503 Service Unavailable</title>
</head><body>
<h1>Service Unavailable</h1>
<p>The server is temporarily unable to service your request due to maintenance
downtime or capacity problems. Please try again later.</p>
</body></html>
```

mysite-error.log журналында келесі жазба пайда болды:

```
[Wed Mar 12 11:44:52.432674 2014] [cgid:error] [pid 13517:tid 139804328126208]
```

(22)Invalid argument:
[client 127.0.0.1:60985] AH01257: unable to connect to cgi daemon after multiple tries:
/home/user/tmp/httpd- install/cgi-bin/getdate

Бұл Apache сервері CGI демонымен байланыса алмай жатқанын білдіреді. Бар блокта ScriptSock директивасын қосайық, ол Apache және CGI демоны байланысуы үшін Беркли сокетіне жол көрсететін болады:

```
<IfModule cgid module>
    #
    #   ScriptSock: On threaded servers, designate the path to the UNIX
    #   socket used to communicate with the CGI daemon of mod cgid.
    #
    Scriptsock /home/user/httpd/logs/cgisock </IfModule>
```

Apache-ні тағы бір рет қайта қосып, бағдарламаны іске қосуға тырысып көреміз. Сервер дәл сол 503 қатені қайтарады. Алайда, журналда енді жаңа жазбаны көруге болады:

[Wed Mar 12 12:01:59.462644 2014] [cgid:error] [pid 16958:tid 139804328126208]
[client 127.0.0.1:33001] Premature end of script headers: getdate

Жазба бұған дейін құрылған CGI-бағдарлама шығарған HTTP тақырыптарының кемшілігі туралы хабарлап тұр. Қажетті тақырыптардың тұжырымын бағдарламаға қосайық. Оның бастапқы коды келесідей үлгіде болады:

```
#!/bin/sh

echo "Content-type: text/plain; charset=iso-8859-1" echo

echo -n "Current server time is " date "+%F %T"
```

Бұл түзетуден кейін Apache серверін қайта қоспастан осы бағдарламаның орындалуын браузерден сұраймыз:

```
user@machine:~/httpd/cgi-bin> curl http://mysite. org:8081/cgi-bin/getdate
Current server time is 2014-03-12 12:05:50
```

Нәтижеге қол жетті. Құрылған CGI-бағдарлама жұмыс істеп тұр.

CGI-дегі сұраныстар параметрі. Web-серверге арналған сұраныстардың көпшілігінде параметрлер жинағы бар. Мысалы, тауарлар тізімін сұрау кезінде пайдаланушы оған тауарларды бағасының төмендеуі бойынша немесе өндірушісі бойынша сұраптау қажет екенін хабарлауы мүмкін. Әдетте, мұндай қосымша талаптар параметрлер түрінде рәсімделеді.

WWW-де URL (UniversalResourceLocator — ресурстар табудың әмбебап құралы) бөлігі болып табылатын сұраныс жолдары ұғымы бар. Онда CGI секілді Web-қосымшаларға жолданатын мәліметтер бар.

URL-дің жалпы бейнесі келесідей:

```
http://server:port/path/?query string
```

Сұраныс жолының негізгі міндеті бастапқыда кейбір өрістері бар HTML-үлгідегі мәліметтер жолдау болатын. Мысалы, жаңа пайдаланушы құру кезінде үлгі келесідей түрде болуы мүмкін:

```
<html>
    <form name="input" action="/cgi-bin/accounts/ad- min/create user"
    method="get">
    First name: <input type="text" name="first name"><br>
    Last name: <input type="text" name="last name"><br> E-mail: <input
    type="text" name="email"><br>
    <input type="radio" name="group" value="dev">developer<br>
    <input type="radio" name="group" value="qa">QA<br><input type="radio"
    name="group" value="viewer">Project viewer<br>
    <input type="submit" value="Create user">
    </form>
</html>
```

<input> тегтері осы үлгінің өрістеріне сәйкес келеді. Сонымен, кезекті пайдаланушыны құра отырып (*Createuser* батырмасын басып*)* келесі сұраныс жолы бар Web-серверге сұраныс жолдайды:

```
first name=Ivan&last name=Petrov&email=ipetrov@ cryptoanalytics.org&group=dev
```

Алайда, бұл жол қолданылған HTTP-әдіске байланысты түрлі тәсілдермен жіберіледі. Мысалды қарастырайық. Пайдаланушыға серверден ағымдағы күнді немесе ағымдағы уақытты сұрауға мүмкіндік беретін қайсыбір үлгі құрайық та, кодты *htdocs/mysite/request. Html* файлға орналастырайық:

```
<html>
    <form name="input" action="/cgi-bin/getdata" method="get">
        <input type="radio" name="format" value="date">Date<br>
        <input type="radio" name="format" value="time">Time<br>
        <input type="submit" value="Send get request"></form>
        form name="input" action="/cgi-bin/getdata" method="post">
        <input type="radio" name="format" value="date">Date<br>
        <input type="radio" name="format" value="time">Time<br>
        <input type="submit" value="Send post request">
        </form>
```

</html>

<form> тегі сұранысты орындау үшін қолданылатын HTTP-әдісті белгілейді.

Осы сұранысты өңдеу үшін Bash-те CGI-скрипт құрайық — *cgi-bin/getdata:*

```
#!/bin/sh
echo "Content-type: text/plain; charset=iso-8859-1" echo
echo "Environment variables:"
env
echo
echo "Input follows:" cat
```

Көрініп тұрғандай, скрипт CGI-бағдарламасы (бұдан әрі – скрипт) үшін орнатылатын барлық айнымалы орталарды шығарады, одан соң скрипт оның стандартты енгізуіне келетіннің барлығын шығарады. Браузерде үлгіні ашамыз *(http://mysite.org:8081/reguest.html)* және екі сұрныстыда орындаймыз — GET пен POST.

GET сұранысы орындау нәтижесінде браузерде мекенжай жолында *http://mysite. org:8081/cgi-bin/getdata?format=date* мекенжай көрсетіледі және келесі тұжырымдама көрсетіледі:

```
Environment variables:
SERVER_SIGNATURE=
HTTP_USER_AGENT=Mozilla/5.0 (X11; Linux x86_64; rv:26.0) Gecko/20100101
Firefox/26.0 SERVER_PORT=8081 HTTP_HOST=mysite.org:8081
DOCUMENT ROOT=/home/user/httpd/htdocs/mysite
LD LIBRARY PATH=/home/user/httpd/lib
SCRIPT FILENAME=/home/user/httpdl/cgi-bin/getdata
REQUEST URI=/cgi-bin/getdata?format=date
SCRIPT_NAME=/cgi-bin/getdata
HTTP_CONNECTION=keep-alive
REMOTE_PORT=50470
PATH=/home/user/bin:/usr/local/bin:/usr/bin:/bin:/
usr/bin/X11:/usr/X11R6/bin:/usr/games:/opt/kde3/bin:/
usr/lib/mit/bin:/usr/lib/qt3/bin
CONTEXT_PREFIX=/cgi-bin/
PWD=/home/user/httpd/cgi-bin SERVER ADMIN=webmaster@mysite.org
REQUEST_SCHEME=http
HTTP_ACCEPT_LANGUAGE=ru,en;q=0.7,en-us;q=0.3
HTTP REFERER=http://mysite.org:8081/request.html
HTTP ACCEPT=text/html,application/
xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
REMOTE_ADDR=127.0.0.1
SHLVL=1
SERVER NAME=mysite.org SERVER_SOFTWARE=Apache/2.4.7 (UNIX)
QUERY_STRING=format=date SERVER_ADDR=127.0.0.1
GATEWAY_INTERFACE=CGI/1.1 SERVER_PROTOCOL=HTTP/1.1
HTTP_ACCEPT_ENCODING=gzip, deflate REQUEST_METHOD=GET
CONTEXT_DOCUMENT_ROOT=/home/user/httpd/cgi-bin/
  =/usr/bin/env

Input follows:
```

Көрініп тұрғандай, стандартты енгізуге ештеңе келмейді (*Inputfollows* секциясы: бос). Алайда, сұраныстың барлық параметрлерін *REQUEST_URI* ортасының айнымалысынан көруге болады.

Браузердің мекенжай жолында барлық параметрлерді сипаттау қызықты факт болып табылады. Үлгісіз, жай ғана *http:// mysite. org:8081/cgi-bin/getdata?format=date* параметрлері көрсетілген URL ашып, дәл осындай нәтиже алуға болады. Ағымдағы сұраныс қай жақтан жолданғанын көрсететін *REFERER* айнымалысы ғана жалғыз айырмашылық болады. Параметрлерді белгілеудің мұндай нұсқасы командалық тәртіпте Web-қосымшаны сұрау кезінде қолайлы (браузерсіз және үлгіні қолданусыз).

POST сұранысын орындап көрейік. Бұл кезде мекенжай жолына сұраныс параметрлері жазылмайды және олар *REQUEST_URI* айнымалыда жоқ болады:

```
Environment variables:
SERVER_SIGNATURE=
HTTP_USER_AGENT=Mozilla/5.0 (X11; Linux x86_64; rv:26.0)
Gecko/20100101 Firefox/26.0 SERVER_PORT=8081 HTTP_HOST=mysite.
org:8081
DOCUMENT_ROOT=/home/user/httpd/htdocs/mysite LD LIBRARY
PATH=/home/user/httpd/lib
SCRIPT FILENAME=/home/user/httpd/cgi-bin/getdata
REQUEST_URI=/cgi-bin/getdata
SCRIPT_NAME=/cgi-bin/getdata
HTTP_CONNECTION=keep-alive
REMOTE_PORT=50641
PATH=/home/user/bin:/usr/local/bin:/usr/bin:/bin:/
usr/bin/X11:/usr/X11R6/bin:/usr/games:/opt/kde3/bin:/
usr/lib/mit/bin:/usr/lib/qt3/bin
CONTEXT_PREFIX=/cgi-bin/
PWD=/home/user/tmp/httpd-install/cgi-bin SERVER ADMIN=webmaster@mysite.org
```

```
REQUEST_SCHEME=http
HTTP_ACCEPT_LANGUAGE=ru,en;q=0.7,en-us;q=0.3
HTTP REFERER=http://mysite.org:8081/request.html
HTTP ACCEPT=text/html,application/
xhtml+xml,application/xml;q=0.9,*/*;q=0.8
REMOTE_ADDR=127.0.0.1
SHLVL=1
SERVER NAME=mysite.org CONTENT_LENGTH=11
SERVER_SOFTWARE=Apache/2.4.7 (UNIX)
QUERY_STRING=
SERVER_ADDR=127.0.0.1
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
HTTP_ACCEPT_ENCODING=gzip, deflate
CONTENT TYPE=application/x-www-form-urlencoded
REQUEST_METHOD=POST
CONTEXT_DOCUMENT_ROOT=/home/user/httpd/cgi-bin/
=/usr/bin/env

Input follows: format=date
```

Бағдарлама тұжырымдамасынан көрініп тұрғандай, орта айнымалысының орнына параметрлер CGI-бағдарламаға стандартты кіруге берілген (*Inputfollows* секциясы*).*

Web-қосымшалардың көпшілігі HTTP-ның белгілі бір әдісіне тіркеусіз жүзеге асырылады, сәйкесінше, бұл үшін клиентпен таңдалған HTML-әдісіне байланысты әртүрлі көздерден сұраныс параметрлерін таңдайтын бірқатар қабат қосу қажет.

Әзірлемеші Крис Джонсон (Chris Johnson) Bash-ке арналған осындай қабатты жүзеге асырудың өз нұсқасын ұсынды. Ол мәліметтерді қолданылған HTTP-әдісіне байланысты таңдады және пайдаланушымен берілген айнымалы параметрлерді санады. Скрипт жұмысының толығырақ түсіндірілуін мына мекенжай бойынша табуға болады: http://www. drdobbs. com/parsing-web-form-input-in-cgi-shell-scri/199103035. Оны құрылған CGI-скриптің бастапқы кодына қосайық және пайдаланушымен сұралған пішімді шығаруға тырысайық:

```
parse query() #@ USAGE: parse query var ...
{
        local  var  val  local
        IFS='&'
        vars="&$*&"
        [ "$REQUEST_METHOD" = "POST" ] && read QUERY_STRING set -f
        for item in $QUERY_STRING do
```

```
        var=$(item%%=*)
        val=$(item#*=)
        val=$(val//+/ } case
        $vars in *"&$var&"* )
                case $val in
                        *%[0-9a-fA-F][0-9a-fA-F]*) printf -v val "%b"
                        "${val//\%/\\x)"

                esac

        esac
        eval "$var=\$val" done set
      +f
)
echo "Content-type: text/plain; charset=iso-8859-1" echo

parse query format
echo "Requested format is the following: $format"
```

Енді екі сұраныс та (POSTи GET) бір нәрсені көрсететін болады, мысалы:

```
Requested format is the following: date
```

Күнмен уақытты көрсетуі үшін скрипті толықтырып жазу ғана қалды:

```
parse query format case $format in
        "date") date +%F;;
        "time") date +%T;;
        *) echo "Error: unknown request - \"$format\""
esac
```

Қате болған жағдайда сервердің журналында сәйкес хабарламалар пайда болады:

```
/home/user/httpd/cgi-bin/getdata: line 35: syntax error near unexpected token 'date'
/home/user/httpd/cgi-bin/getdata: line 35: ' date) date +%F;;'
```

Осылайша, бағдарламалаудың кез-келген тілінде CGI интерфейсі арқылы Web-қосымша жазуға болады:

```
user@machine:~/httpd/cgi-bin> curl http://mysite.
org:8081/cgi-bin/getdata?format=time
11:40:32
user@machine:~/httpd/cgi-bin> curl http://mysite.
org:8081/cgi-bin/getdata?format=date
2014-03-13
user@machine:~/httpd/cgi-bin> curl http://mysite.
org:8081/cgi-bin/getdata?format=qqq
```

Error: unknownrequest — "qqq"

PHP. Бұл серверде түсіндірілетін және орындалатын HTML-ге кіріктірілетін скрипт-тіл *(scriptinglanguage)*. Ең дұрысы мысал арқылы көрсету болады:

```
<html>
<head>
<title>Example</title>
</head>
<body>
<?php echo "Hi, I'm a PHP script!"; ?>
</body>
</html>
```

Бұл скрипті орындағаннан кейін мына жазбасы бар HTML-парақша пайда болады:

```
Hi, I'm a PHP script!
```

Perl немесе C секілді басқа тілдерде жазылған CGI-скриптерден айырмашылығы — бұл CGI-бағдарламаларда парақшаның толық HTML-кодын жасау керек болады, ал PHP қолданса — ашатын және жабатын тегтерді қолдана отырып, дайын HTML-парақшаға бағдарламаны орнатса жеткілікті (мысалы, <?php и ?>).

Ресурстарды тұтынуды басқару. Ресурстарды тұтынуды басқару көзқарасы бойынша мұндай Web-қосымшаларды Apache модульдері аясында, яғни, Apache-нің жеке өз процестерінде және оның есептік жазбасы атынан іске қосылатындар және сұраныстарды Web-серверден оқшау орындайтындар деп бөлуге болады.

Apache модульдерінің аясындағы Web-қосымшалардың жұмыстарын қарастырайық. Ең кең таралған мысалдардың бірі – *mod_php,* ол PHP тілінде код түсіндірушісінің жұмысын іске асырады. Сұранысты өңдеу процесінің орындалуы кезеңі шамамен келесідей:

1) Apache-нің ағымдағы процесіне сұраныс келеді;
2) PHP түсіндірушісі сұранысқа сәйкес кодты компиляциялайды және орындайды;
3) Apache процесі клиентке бағдарлама жұмысының нәтижесін жолдайды;
4) Apache процесі өз жұмысын аяқтайды (кейбір жағдайларда ол келесі сұраныстарды өңдеу үшін өз әрекетін жалғастыруы мүмкін, бірақ, бұл міндетті емес).

Осылайша, мұндай бағдарламаның өзіне тән мынадай қсиеттері бар:

- бағдарлама Apache процесінде орындалады, сәйкесінше, оның ресурстары осы процестің ресурстарымен шектелген. Apache үшін ресурстардың шектелуі жайында бұған дейін айтылды;

- бағдарлама аяқталған соң өзінің барлық ресурстарын босатады, себебі, процесс аяқталады.

Бұл қасиеттер Web-сервердің ресурстарымен оларды шектей отырып, Web-қосымшаның ресурстарын толыққанды басқаруға мүмкіндік береді.

JavaScript. Web-парақшалардың HTML-кодын қарапайым генерациялаудан басқа серверде HTML базасында әлдеқайда интерактивті қосымша құру әдісі бар, бұл JavaScript бағдарламалау тілін қолданумен жүзеге асырылады. Бұл тіл HTML-дің соңғы сипаттізімдерінде сипатталған, жазу кезінде оның ішіндегі ең соңғы нұсқасы HTML 5 болатын.

JavaScript графикалық интерфейс элементтерімен түрлі әрекеттер орындауға мүмкіндік береді: терезелер, диалогтар, енгізу жолдарын құру, пайдаланушылардың әрекеттерін интерактивті өңдеу. JavaScript-те жазылған заманауи қосымшалар пайдаланушы интерфейсінің ыңғайлылығы жағынан C/C++, Java және тағы басқа тілдерде жазылған дәстүрлі компиляциялынған қосымшалардан кем түспейді.

Осылайша, пайдаланушымен көрсетілетін браузер терезесіндегі нысандар Web-серверде туындауы да, браузерде HTML-парақшасының кодын орындау процесі кезінде құрылуы/түрленуі мүмкін.

Пайдаланушы интерфейсі бар операциялардан басқа JavaScript көптеген өзге де операцияларды орындай алады, мысалы, мәліметтер алмасу және есептеу. Мәліметтер алмасу үшін көп жғдайда AJAX (Asynchronous JavaScript and XML — асинхронды JavaScript пен XML) технолгиясы қолданылады, ол браузерде Web-сервермен қосымшаның мәліметтерін фондық алмасу үшін қолданылады. Бұл технологияның жұмысы нәтижесінде бүкіл HTML-парақшаны қайта жүктеу қажеттілігі жоғалады, ал оның орнына оның тек бір үзіндісі ғана қайта салынады.

AJAX технологиясының келесідей артықшылықтары бар:

- *трафик үнемдеу.* AJAX-ты қолдану Web-қосымшамен жұмыс кезінде трафикті айтарлықтай қысқартуға мүмкіндік береді, бұл бүкіл парақшаны жүктеудің орнына тек өзгертілген бөлігін ғана жүктеудің немесе JSON немесе XML үлгісінде мәліметтер жинағын алып/жіберіп, содан соң парақшаның ішіндегіні JavaScript арқылы өзгертудің арқасында орын алып отыр;
- *серверге жүктеменің азаюы.* AJAX-ты дұрыс іске асыру кезінде серверге жүктемені айтарлықтай төмендетуге болады. Негізінен, сайттың барлық парақшаларын бір үлгі бойынша өндіріледі, бұл генерация үшін түрлі файлдарға жүгінуді талап ететін өзгермейтін элементтер («тақырыбы», «навигациялақ панель», «белдеме» және т.б.), скриптерді өңдеуге арналған уақыт (кейде мәліметтер базасына арналған сұраныстар) – егер, парақшаны толық жүктеуді тек мазмұнды бөліктің генерациясы және жолдануымен алмастырса, мұның барлығын орындамауға болады. Парақша дизайны да әдетте оларды

қайтадан өңдеу үшін AJAX қолданып, уақыт жұмсауды талап етпейтін рәсімдеумен байланысты көптеген файлдарды қамтиды (HTPP-қосылуларының санын үнемдеу олардың әрқайсысына трафик қысқартудан пайдалырақ);

- *интерфейс реакциясын жылдамдату.* Өзгерген бөлікті жүктеу айтарлықтай жылдам болғандықтан, пайдаланушы өз әрекеттерінің нәтижесін өте жылдам және парақшаның жарқ етуінсіз (толық жүктеу кезінде пайда болады) көре алады;
- *интерактивті өңдеуге арналған үлкен мүмкіндіктер.* Мысалы, Google-ге іздеу сұранысын енгізу кезінде сұрансыстың ұқсас нұсқалары бар көмекші нұсқалар шығарылады. Көптеген сайттарда тіркеу кезінде пайдаланушы есімді енгізеді де, ол есім қолжетімді ма, жоқ па, оны бірден көреді. AJAX уақыт өте келе өзгеретін мәліметтерді шығаратын чаттарды, әкімшілік панельдерді және басқа да құралдарды бағдарламалау үшін қолайлы.

AJAX арқылы сұраныстар жолдау кезінде клиент парақша фрагменттерін емес, осы фрагментті толықтыруға арналған мәліметтерді жиі сұрайды. Осылайша, браузер мен Web-сервер HTML + JavaScript-те жазылған қосымшаны түгел жүктеген соң, бір-біріне тек кейбір нысандарды ғана жолдап отырады. Бұл нысандарды DTO (Data Transfer Object — мәліметтер жолдауға арналған нысандар) деп атау қабылданған.

JavaScript бастапқы коды мен қосымшалар сервері арасындағы DTO нысандарды синхрондауда проблема бар, бұл Web-қосымшалар JavaScript-тен басқаша бағдарламалау тілінде жазылуына байланысты туындайды. *Google* корпорациясы қызықты технология — GWT (Google Web Toolkit — *Google* компаниясынан Web-ке арналған құралдар*)* әзірледі, ол браузер үшін Java тілінде код жазып, содан кейін оны JavaScript кодына компиляциялаувға мүмкіндік береді. Бұл үш буынды қосымшаның клиент және сервер тараптарында кодтың жартысын Java-да қолдануға мүмкіндік туғызады. Ал бұл мәселе өз кезегінде әзірленетін бағдарламалық өнімнің сүйемленденуін айтарлықтай жеңілдетеді.

1.12. МӘЛІМЕТТЕР БАЗАСЫМЕН ӨЗАРА ӘРЕКЕТТЕСУ

Заманауи Web-қосымшалар түрлі мәліметтер базасына пайдаланушы интерфейсін ұсыну үшін жиі қолданылады. Көпбуынды қосымшалардың концепциясын қарастырайық.

Көпбуынды қосымша — бұл мәліметтер ұсыну, өңдеу және сақтау нақты таратылатын клиент-серверлі архитектура. Көпбуынды қосымшалар кеңінен таралды. Оларда пайдаланушылар интерфейсі, функциялық логика (бизнес-логика), мәліметтер сақтау және мәліметтерге қолжетімділікті

шектеу түрлі модульдермен жүзеге асырылған және жиі жағдайда түрлі аппараттық платформаларға бөлінген.

Модульдер арасындағы нақты ұйымдастырылған өзара әрекеттестігі бар қарапайым модульдік архитектураға қарағанда үшбуынды қосымша әрбір бөліктің басқаға тәуелсіз өзгеруін немесе жаңаруын білдіреді. Мысалы, пайдаланушылық ұсыну деңгейінде ОЖ өзгеруі тек пайдаланушы интерфейсінің бастапқы кодына ғана әсер етеді.

Әдетте, пайдалоанушы интерфейсі ДЭЕМ-де немесе жұмыс станциясында іске асырылған және стандартты графикалық интерфейсті қолданады. Функциялы логиканың буыны біәрнеше модульдерден тұруы мүмкін және жұмыс станциясында немесе қосымшалар серверінде орындалады. Мәліметтер сақтау буынында мәліметтер базасының серверінде орналасқан мәліметтер базасын басқарудың реляциялық жүйесі болады.

Негізі, үшбуынды архитектурада келесі буындарды атап көрсетеді:

1) *пайдаланушылық ұсыну буыны.* Бұл қосымшаның ең жоғарғы қабаты (буыны). Бұл буын пайдаланушыға оған ыңғайлы түрде мәліметтерді ұсынады. Әдетте, бұл буын пайдаланушының интернет-браузері деп танылады;
2) *қосымшалар буыны.* Бұл қосымшаның бизнес-логикасы орындалатын, сондай-ақ, қолжетімділікті шектеу қолданылатын логикалық буын;
3) *мәліметтер буыны.* Ол қосымшалар буынына өңдеуге арналған мәліметтерді ұсынатын мәліметтер базасының серверлерінен тұрады. Бұл буынды бөлу жүйенің масштабталуын ұлғайтуға мүмкіндік береді.

Пайдаланушылық ұсыну буынына арналған ең кең таралған платформа интернет-браузер болып табылады, қосымшалар буынымен өзара әрекеттестік HTTP хаттамасымен жүзеге асырылады. Бұл архитектурада барлық буындар тек көршілес буындармен ғана байланысты екенін түсіну керек, яғни, пайдаланушы интерфейсінің мәліметтер қоймасына тікелей қолжетімлігі болмауы керек. Осылайша, қосымшаны жобалау кезінде мәліметтер базасымен өзара әрекеттестік қосымшалар серверінен ғана орындалады.

Парақшалар құрудың негізі идеясы мыналардан тұрады:

- HTML-парақшада тақырып, мәліметтер және соңы ерекшеленеді;
- CGI тұжырымдамасына тақырып қойылады;
- дайындалған үлгіге мәліметтер буынынан келген мәліметтер қосылады;
- құжат соңы қосылады.

Әрине, түрі айтарлықтай күрделі HTML-парақшалар құруға да болады. Bash-тағы CGI-бағдарлама үлігісінде LDAP мәліметтер базасынан барлық пайдаланушылар тізімін шығаратын қосымша мысалын қарастырайық. Пайдаланушының топтар тізімін пайдаланушы идентификаторы бойынша

қайтаратын қызмет құрайық:

```
get user groups() {
        local useruid=$1;
        local groups='ldapsearch -Q -LLL
        "(&(objectClass=inetOrgPerson)(uid=$useruid))" memberOf \
            | grep "^memberOf:" | cut -d ":" -f 2 | sed 'M's/^A.*cn=\([a-z-
        ]*\).*$/\1/" echo $groups
}
```

Оның бүкіл параметрлерін біріктіретін қызметті үтір арқылы қосайық (*IFS* арнайы айнымалыны қолданумен):

```
print fields() { local IFS="," echo -n "$*"
}
```

HTML-парақшаның тақырыбы *echo* және *cat* командаларының көмегімен түрленетін болады:

```
echo Content-type: text/html echo
cat <<EOF <html>
    <table>
        <tr>
        <th>user ID</th><th>Full name</th><th>E-mail</ th><th>groups</th>
        </tr>
EOF
```

LDAP-тағы posixAccount нысандарының жергілікті айнымалы атрибуттеріне жүктеп, LDAP-тағы барлық пайдаланушыларды сұраймыз:

```
ldapsearch -LLL -Q objectClass=inetOrgPerson uid | grep "^uid: " | cut -d " " -f 2 | sort | \
while read useruid; do values='ldapsearch -Q -LLL
        "(&(objectClass=inetOrgPerson)(uid=$useruid))" \
            | sed "s/\(\w*\): \(.*\)$/\1=\"\2\"/"" unset cn
        unset displayName unset mail eval $values
        echo -n "<tr><td>$uid</td><td>$displayName</
        td><td>$mail</td><td>";
        print fields 'get user groups $useruid'
         echo "</td></tr>
done
```

Одан әрі парақшаның соңын толықтырып жазу керек.

БАҚЫЛАУ СҰРАҚТАРЫ

1. Web-сервер деген не? HTTP хаттамасы не үшін қолданылады?
2. Әдетте Web-серверлер қандай TCP-порттарды қолданады? Олар басқа TCP-порттарды қолдана алады ма?
3. Сервердің түбірлік директориясы деген не? Ол серверді баптауда қалай қолданылады?
4. Web-сервердің өнімділігін ұлғайту үшін қандай негізгі әдістер қолданылады?
5. Директория индексі деген не?
6. Web-сервердің конфигурация файлында директиваның көріну аумағы қалай белгіленеді?
7. Apache Web-серверінің резервтік көшірмелеу қалай жүргізіледі? Apache-де конфигурация файлдарың өзгерістерін бақылау қалай жүзеге асырылады?
8. Түрлі ОЖ-дағы Apache-ді қосу, тоқтату және қайта қосу қалай жүзеге асырылады?
9. Бірнеше тораптар хостингі немесе виртуаллды хостинг дегеніміз не? Виртуалды хостингтің қандай түрлері бар?
10. Виртуалды тораптардың журналдарын бір-бірінен қалай ажыратуға болады?
11. Порттар немес IP-мекенжайлар бойынша виртуалды хостингті баптау үшін қандай директивалар қолданылады?
12. IP-мекенжайлар бойынша виртуалды хостингтің баптаулары серверлер атауы бойынша хостингтен қандай директивалармен ерекшеленеді?
13. Пайдаланушылардың үй парақшалары дегеніміз не?
14. Web-сервер Интернеттен қолжетімді болуы үшін қандай әрекеттер орындау керек?
15. Web-сервера журналдарының файлдары қайда болады? Олар қалай бапталады?
16. Географиялық тұрғыдан Web-серверді қайда орналастырған дұрыс?
17. Web-сервер порты ашық екенін қалай тексеруге болады?
18. Web- сервердің HTTP-сұраныстарға жауап беріп жатқанын автоматты (консольден) түрде тексеруге болады?
19. Web- сервер жұмысы статистикасының шұғыл мәндерін қалай алуға болады?
20. Web-сервер директорияларына қолжетімділік қалай шектеледі?
21. Директорияларға қолжетімділікті шектеу директорияларының көріну аумағы қандай?

22. Автоматты индекстеу деген не? Оны не үшін және қалай қосуға/сөндіруге болады?
23. Ашық кілт (PKI) инфрақұрылымы не үшін қолданылады?
24. Apache HTTP Server үшін өздігінен қол қойған сертификатты қалай әзірлеуге болады?
25. Өздігінен қол қойған сертификаттың кемшіліктері қандай?
26. Үдемелі Web-парақшалар деген не?
27. Үдемелі Web-парақшалар үшін қандай технологиялар кең таралған? Олардың артықшылықтары мен кемшіліктері неде?
28. Мәліметтер базасымен өзара әрекеттестік қалай жүзеге асырылады?
29. AJAX технологиясының мәні неде? Оның артықшылықтары мен кемшіліктері қандай?
30. *mod_rewrite* сұранысының қайта жазу модулі не істейді?

2 бөлім

БРАНДМАУЭРДІ ОРНАТУ ЖӘНЕ ПАРАМЕТРЛЕРІ

2.1. БРАНДМАУЭРДІҢ НЕГІЗГІ ФУНКЦИЯЛАРЫ

Брандмауэр (brandmauer), немесе *желілік экран,* — желіні бірнеше бөлікке бөлуге және оның бөліктері арасында ақпараттың өтуі үшін арналған шарттарды анықтайтын ережелер жинағын жүзеге асыруға мүмкіндік беретін бағдарламалық және аппараттық құралдар жинағы.

«Брандмауэр» термині неміс тілінен кіріктірілген және ағылшынның «firewall» түпнұсқалық мәніндегі баламасы болып табылады (өрттің таралуының алдын ала отырып, іргелес ғимараттарды бөлетін қабырға). Компьютерлік технологиялар облысында неміс тілінде «firewall» сөзінің қолданылатындығы қызық.

Желілік экранның негізгі міндеті компьютерлік желілер немесе бөлек түйіндерді рұқсат етілмеген қолжетімділіктен қорғау болып табылады. Желілік экрандарды сүзгілер деп те атайды, себебі олардың негізгі міндеті — кескіндемеде анықталған критерийлерге сәйкес келмейтін қалталарды өткізбеу (сүзгілеу).

Кейбір желілік экрандар да *мекенжайларды көрсетуді* — желішілік (сұр) мекенжайларды немесе порттарды локалды есептеуіш желіден тыс қолданылатын сыртқыларға динамикалық ауыстыруды жүзеге асыруға мүмкіндік береді.

Брандмауэрлер — бұл ОЖ-мен күрделілігі бойынша салыстырылатын жүйелер классы. Олар орындалуы бойынша классификацияланы мүмкін: аппараттық, бағдарламалық, аралас типті; компоненттік моделі бойынша: үлестірілген және жергілікті. Бірақ ең пайдалысы — бұл брандмауэрлер әрекет ететін деңгей бойынша классификация: қолданбалы, қалталық және байланысу деңгейі.

Деңгейлер бойынша осылай бөлу — бір бөлек брандмауэрдің бір деңгейден көп деңгейде бір уақытта жұмыс істеу мүмкіндігін білдіретін шартты болып табылады. Барлық дерлік брандмауэрлердің функционалдылықты кеңейтуге және қандай да бір сұлбада жұмыстың артықшылықтарын максималды пайдалануға ұмтыла отырып, бірнеше деңгейде әрекет ете алатындығын ерекшелеуге болады. Мұндай технология Stateful Inspection деп аталады, ал аралас сұлба бойынша жұмыс істейтін — Stateful Inspection Firewall деп аталады.

Мінсіз брандмауэр алты функцияны орындауы тиіс.

1. *Сыртқы шабуылдарды бұғаттау бойынша жұмыс.* Брандмауэрлар шабуылдардың барлық типтері бұғатталуы тиіс, сонымен бірге онда порттарды сканерлеу, құпиясөздерді іріктеу, IP-спуфинг және т.б.

2 *Кез-келген ақпараттың шығып кетпеуін бұғаттау.* Қауіпті кодтың желі арқылы, сайттан (ddos қорғауы бар хостингтегі серверді жалға алу жүзеге асырылған) немесе сатып алған пираттық CD вирус түрінде кіруі болсын — брандмауэр ақпараттың шығып кетуінің алдын алуы тиіс, вирустың желіге шығуы бұғатталуы тиіс.

3. *Қолжетімділіккке рұқсатты сұратып жатқан қосымшаларды бақылау.* Қосымшалар сайттардан шығуы мүмкін (Украинадағы хостингті пайдалана отырып, серверді жалға алу рәсімделуі мүмкін). Брандмауэр файлдың аты

бойынша тексеру, сонымен бірге оның түпнұсқалылығын тексеру жүзеге асырылуы тиіс.

4. *Аймақтық қорғанысты қолдау.* Жиі локалды желіде жұмыс істеу барлық локалды контентке толық сенім білдіруді де білдіреді. Осылайша, потенциалды қауіпті болатын ең жаңа технологияларды пайдалануға арналған бірегей мүмкіндіктер ашылуы мүмкін. Сондықтан олардың құрамының қауіптілігін талдауды жүргізуге деген дифференциялданатын тәсілдеме қамтамасыз етілуі тиіс.
5. *Алдын алу және протоколдау.* Ақпарат көлемі артықшылықсыз немесе кемшіліксіз жиналуы тиіс.
6. *Жұмыстың максималды айқындығы.* Жүйе баптауының күрделілігі оның тиімділігін білдірмейді. Жүйе баптауының күрделілігі оның тиімділігін білдірмейді. Баптау үшін «шеберлерді» қолдануды ескермеуге болмайды, себебі бұл уақытты айтарлықтай үнемдеуге мүмкіндік береді.

2.2. БРАНДМАУЭР ТИПТЕРІ

OSI (Open Systems Interconnection Basic Reference Model — ашық жүйелердің өзара әрекеттесуінің базалық эталондық моделі) желілік моделі қолдайтын деңгей желіаралық экрандарды бөлу кезіндегі негізгі сипаттама болып табылады. Желіаралық экрандардың келесі типтері бөлінеді:

1. *Басқарылатын коммутаторлары* (арналық деңгей).
2. *Желілік деңгейдегі желілік сүзгілер* (stateless). Статикалық сүзгілеу, дереккөз бен қабылдаушы, протокол, жіберуші мен қабылдаушының порттарының IP-мекенжайын талдау жолымен жүзеге асырылады.
3. *Сеанстық деңгей шлюздері* (circuit-level proxy). TCP/IP желілік моделінде бір ауыздан OSI сеанстық деңгейіне сәйкес келетін деңгей жоқ, сондықтан сеанстық деңгей шлюздарына желілік деңгеймен де, машиналық деңгеймен де, қолданбалы деңгеймен де теңдестіру мүмкін болмайтын сүзгілерді жатқызады:

- тарататын мекенжайлар (NAT, PAT) немесе желілік протоколдарды (тарататын көпір), шлюздер;
- арна жағдайын бақылау сүзгілері. Байланыс арнасының жағдайын бақылау сүзгілеріне жиі пакеттердің тақырыпаттарын қосымша талдайтын және үзінділенген пакеттерді сүзгілей алатын кеңейтілген мүмкіндікті желілік деңгейлі желілік сүзгілер (stateful)жатқызылады;
- сеанстық деңгей шлюздері. Сеанстық деңгейдің ең танымал және мәлім шлюзі SOCKS делдалы болып табылады;

Қолданбалы деңгейлі шлюздер (application-level proxy), жиі прокси-серверлер деп аталады. Ашық (transparent) және ашық емес болып бөлінеді.

SPI брандмауэрі(Stateful Packet Inspection), немесе *пакеттерді динамикалық сүзгілеуші брандмауэрлер* (Dynamic Packet Filtering). Негізінен кеңейтілген мүмкіндіктері бар сеанстық деңгей шлюздері болып табылады. Жағдай инпекторлары сеанстық деңгейде пайдаланады, бірақ қолданбалы және желілік деңгейдегі протоколдарын «түсінеді». Әрбір қосылыс үшін TCP екі виртуалды арнасын ашатын (біреуі – клиент үшін, біреуі – сервер үшін) қолданбалы деңгейлі шлюзбен салыстырғанда жағдай инспекторы клиент пен сервер арасындағы тура байланысты ұйымдастыруға кедергі жасамайды.

2.3. ФАЕРВОЛ ШЕШПЕЙТІН МӘСЕЛЕЛЕР

Фаервол (брандмауэр, жеке желіаралық экран) өздігінен желі үшін барлық қауп-қатерден қорғаудың әмбебап құралы болып табыламайды:

- желі түйіндерін «есікшелер» (back doors)арқылы өтіп кетуден немесе бағдарламалық қамсыздандырудың әлсіздігінен қорғамайды
- көптеген ішкі қауіп-қатерден, ең алдымен – мәліметтердің шығып кетуінен қорғанысты қамтамасыз етпейді;
- пайдаланушылардың зиянды бағдарламаларды жүктеуінен, соның ішінде вирустардан қорғамайды.

Соңғы екі мәселені шешу үшін сәйкес қосымша құралдар, негізінен антивирустар қолданылады. Әдетте олар фаерволға қосылады және өзге прокси желілік түйіндері үшін мөлдір ретінде жұмыс істей отырып өзі арқылы желілік трафиктің сәйкес бөлігін өткізеді, немесе фаерволдан барлық жіберілетін мәліметтердің көшірмесін алады. Алайда мұндай талдау үлкен аппараттық ресурстарды талап етеді, сондықтан әдетте желінің әрбір түйінінде өз бетінше жүргізіледі.

2.4. FIREWALL ЖҮЗЕГЕ АСЫРЫЛУЫ

Желіаралық экранды таңдау кезінде екі критерий – сенімділік пен ыңғайлылықты басшылыққа алу қажет. Соңғысына қатысты айтатын болсақ, брандмауэрдің бұл сипаттамасы өте субъективті болып табылады. Әрбір адам қолдануды қарапайым болатын желіаралық экранды таңдауды немесе көптеген режимдері бар экранға тоқталуды өзі үшін өзі шешуі тиіс. Бірақ тағы да бір маңызды критерий — бұл брандмауэр қамтамасыз ететін қорғаныстың сенімділігі. Қандай да бір кандидаттың желілік қауіп-қатерді қаншалықты жақсы жеңіп шығып жатқандығын анықтау үшін компьютердегі сыни жағдайға ұқсататын әр түрлі тесттерді жүргізу қажет. Басты мақсаты брандмауэр сенімділігін тексеру болып табылатын көптеген жобалар бар. Уақыт өте келе мұндай егжей-тегжейлі тестілеудің нәтижелері жалпыға қолжетімді болады, және оларды Желіде кедергісіз табуға болады. Қазіргі уақытта мәліметтердің шығып кетуіне тестілердің ең жақсы көрсеткіштері Comodo Firewall брандмауэріне тиесілі болып табылады. Алайда жағдайдың өте жылдам өзгеруі мүмкін екендігін есте сақтау керек, себебі компьютерге зиян келтірудің жаңа тәсілдері күн сайын пайда болады емес пе. Сондықтан өзіңіздің брандмауэріңізді мүмкіндігінше жиі жаңартып тұруды ұмытпаңыз.

Өзінің мәні бойынша Firewall ОЖ-мен өте тығыз байланысты, сол үшін ең кең таралған үш ОЖ: Windows, Linux және MAC OS үшін ең танымал Firewall қарастырайық.

Windows арналған Firewall. *Windows брандмауэрі* — MS Windows кіріктірілген желіаралық экраны. Windows XP SP2 пайда болды. Бастамашысынан (Internet Connection Firewall)айырмашылықтарының бірі бағдарламалардың желіге қолжетімділігін бақылау болып табылады. Windows брандмауэрі Windows Қауіпсіздікті қамтамасыз ету орталығының бір бөлігі болып шығады.

Windows Vista брандмауэрге оны корпоративті ортада ашуды жақсартатын

жаңа мүмкіндіктерді қосады:

- *Windows брандмауэрі* консолінің қосымша мүмкіндіктерге қолжетімділікті алуға мүмкіндік беретін, сонымен бірге қашықтан әкімшілік етуді қолдайтын жоғары қауіпсіздік режиміндегі жаңа жабдықталуы. Оған қолжетімділікті *Іске қосу / Басқа панелі / Әкімшілік ету / Жоғары қауіпсіздік режиміндегі Windows брандмауэрі* арқылы немесе *wf. msc* командасы арқылы алуға болады*;*
- IPv6 қосылыстар сүзгісі;
- вирустар мен тыңшылық бағдарламалық қамсыздандырумен күресуге мүмкіндік беретін шығыс трафикті сүзгілеу. Сүзгілеуді MMC басқару консолін пайдалана отырып баптауға болады;
- IP-мекенжайлар мен порттардың белгілі бір диапазондарына қатысты ережелерді қолдану мүмкіндігін беретін пакеттердің кеңейтілген сүзгісі;
- қызметтің толық атауын көрсету қажеттілігінсіз тізімнен қызметтердің атауларын пайдалана отырып, қызметтерге қатысты ережелерді ұсыну мүмкіндігі;
- қауіпсіздік сертификаттарына, Kerberos сәйкестендіруіне және т.б. негізделген қосылыстарды сүзгілеуге мүмкіндік беретін IPsec толық интгерациялау. Шифрлеуді қосылыстың кез-келген типі үшін талап етуге болады;
- желілік профильдерді жақсартылған басқарылуы (үй, жұмыс және көпшілік желілер үшін әр түрлі ережелерді қалыптастыру мүмкіндігі). Домен мен серверді оқшаулау саясатын сақтауды қамтамасыз ететін ережелерді қалыптастыруды қолдау.

Болашақта брандмауэр қағидалық дамуға қол жеткізбеді.

Comodo Internet Security — американдық компания әзірлеген тегін Firewall. Ол рейтингтегі көшбасшы орынға бірінші жыл ие болып келе жатқан жоқ. Бұл Firewall қоса троян мен басқа вирустардан қорғанысты қамтитын кешенді шешім. Бағдарламада әр түрлі баптаулардың көп мөлшері бар. Ақылы нұсқасында компьютерді қорғау, оңтайландыру және баптау бойынша және сымсыз қосылыстар арқылы таратылатын мәліметтерді шифрлеу бойынша қосымша функцияларға ие. Өкінішке орай, орысша нұсқасы жоқ.

Agnitum ресейлік компаниясының *Outpost Security Suite* — ең кең танымал Firewall (ұзақ уақыт бойы рейтингтегі бірінші орынға ие болған) бірі. Outpost Security Suite — вирустар, трояндар, шпиондық бағдарламалардан қорғанысты, қосымшаларды бақылауды, спамнан қорғанысты, жағымсыз жарнаманы бұғаттауды, жағымсыз парақшаларға кіруден қорғанысты және т.б. қамтитын кешенді шешім. Бұл ең жақсы және сенімді шешімдердің бірі. Баптаулардың мүмкіндіктері кішкене қысқартылған тегін нұсқасы да, ақылы нұсқасы да бар.

Privatefirewall — американдық компания (ресейлік бағдарламалаушылармен белсенді түрде бірге қызмет ететін) әзірлеген, компьютерді қорғау бойынша кешенді шешім. Privatefirewall әр түрлі қауіп-қатерлер типінен қорғанысты қамтамасыз етеді, алайда зарарлы компьютерді өз бетінше емдей алмайды, сол үшін оны антивирустық бағдарламалық қамсыздандырумен бір жиынтықта қолдану ұсынылады. Әзірге орысша нұсқасы жоқ.

Kaspersky Internet Security — антивирустық бағдарламалық қамсыздандыруды әзірлеу облысындағы лидер – Касперский Зертханасынан компьютерді кешенді қорғауға арналған шешім. Пайдаланушылардың тестілері мен пікірлеріне сәйкес көптеген параметрлер бойынша сенімді қорғанысты қамтамасыз етеді (Firewall рейтингтінде де, внтивирустар рейтингінде де ең жақсылардың бірі). Бұл ретте Kaspersky Internet Security қолданылуында және баптауында да көптеген

баламалармен салыстырғанда өте қарапайым. Осындай бағдарламалар үшін дәстүрлі ьолып табылатын модульдерден бөлек антифишинг, ата-аналық бақылау және т.б. секілді қосымша функцияларды қамтиды. Авторлық баға бойынша Kaspersky Internet Security пайдаланушылардың көбісі үшін (әсіресе «тәжірибелі емес») ең жақсы таңдау болып табылады.

SpyShelter Firewall — Datpol поляк компаниясы әзірлеген, үй компьютерін қорғауға арналған өте қарапайым және ыңғайлы шешім. Өзінің антивирустық модулі жоқ, Virus Total интернет-қызметі арқылы күдікті файлдарды тексере алады. Орысша нұсқасы бар.

Келесі брандмауэрлер бірнеше рет тестіленген және қолдануға ұсынылмайды: Jetico Personal Firewall, ESET Smart Security, ZoneAlarm Extreme Security, ZoneAlarm Free Antivirus + Firewall, avast! Internet Security, Total Defense Internet Security Suite, eScan Internet Security Suite, Dr. Web Security Space, Webroot Secure-Anywhere Complete, Avira Internet Security, K7 TotalSecurity, Norton Internet Security, TrustPort Total Protection, Bitdefender Total Security, PC Tools Internet Security, FortKnox Personal Firewall, ThreatFire, ArcaVir Internet Security, G Data TotalProtection, Norman Security Suite PRO, Ad-Aware Total Security, AVG Internet Security, BullGuard Internet Security, F-Secure Internet Security, McAfee Total Protection, Panda Global Protection, Rising Personal Firewall, UnThreat Internet Security, AhnLab V3 Internet Security, VIPRE Internet Security.

Mac OS арналған Firewall. Mac OS үшін көптеген Firewall бар: Mac OS-не кіріктірілген, ақылы, тегін, кешенді қорғаныс жүйелеріне кіріктірілген және т.б.

Mac OS желілік қорғанысының ең танымал құралдарының кішкене шолуын жүргізейік.

Application Firewall (Apple Inc.) кіріс қосылыстарын қорғайды. Бұл қосымшалардың Mac OS кіріктірілген брандмауэрі.

Ipfw (Apple Inc.) желілік трафикті толық бақылауды жүзеге асырады. Бұл өте кең функциялар жинағы бар кіріктірілген күшті желіаралық экран болып табылады. Бәлкім, Mac OS арналған ең жақсы Firewall болар, бірақ барлық баптау командалық қатардан жүргізіледі, ал бұл Mac OS әкімшілеу облысындағы кәсіпқойларға ғана қолжетімді болып табылады.

DoorStop X Firewall (OpenDoor Networks) — тек кіріс қосылыстарды ғана бақылайтын, жүйені қорғауға арналған қосымша, бұл DoorStopX ipfw қондырмасы болып табылатынына қарамастан, оны Mac OS кіріктірілген Application Firewall ұқсас етеді.

IPNetSentryX (Sustainable Softworks) — өте күшті ақылы Firewall, өзінің Network Kext қолданады. Желілік трафикті толық бақылауды қамтамасыз етеді. Құрамында трафик инспекторы, whois, trace, lookup, логтарды қадағалау, TCP dump және тіпті IDS (Intrusion Detection System — күшпен енуді анықтау жүйесі)кейбір ұқсас секілді қосымша утилиттер жинағы болады. Шабуылдаушы хостты автоматты түрде бұғаттау мүмкіндігі бар өте икемді қорғау жүйесін қалыптастыра отырып, иерархиялық түрде ұсынуға болатын ережелердің өте ыңғайлы және логикалық редактор. Құрамында хостты шабуылдардың өте көп таралған түрлерінен қорғау үшін жеткілікті «үнсіз келісім бойынша» ережелер жжинағы болады.

Ыңғайсыздықтары ішінен мәзір қатарына жылжытылмайтын фаервол қабықшасының тұрақты түрде жұмыс істеуінің қажеттілігін ерекшелеуге болады.

Little Snitch (Objective Developmen) — шығыс қосылыстарды бақылауды жүзеге асыратын ақылы Firewall. Apple кіріктірілген Application Firewall бірге үй пайдаланушысы үшін жеткілікті деңгейде компьютерді қорғауды қамтамасыз етеді.

Internet Security Barrier X6 (Intego) — келесі функцияларды қосымша жүзеге асыру есебінен қорғаудың кешенді жүйесін жүзеге асыратын ақылы Firewall: антивирус, антишпион, кіріс және шығыс қосылыстарды бақылау, антифишинг, антиспам, контентті бақылау (ата-аналық бақылау), резервтік көшіру, Data Guard (деректерді қорғау). Әр түрлі қауіп-қатерлер типінен қорғауға арналған утилиталар жинағы ғана емес, компьютердің белсенділігіне мониторинг жасаудың әр түрлі құралдарын ұсынатын бірінші санатты жеке қорғаныс жүйесі бар.

Әр түрлі қызметтерді баптаудың икемді ережелері қолдану қауіпсіздігі мен ыңғайлылығы арасындағы қажетті теңгерімге қол жеткізе отырып, қорғану ережелерін өте жұқа баптауға мүмкіндік береді.

Әр түрлі трояндар (залалсыз сыртқы түрімен немесе қандай да бір саналы функционалы бар бағдарламалар түрінде пайдаланушының компьютеріне енетін және залал келтіретін зиянды бағдарламалар, бұл кредиттік карталар нөмірлері секілді жеке ақпаратты троянды әзірлеушіге беру немесе зарарлы машинаны қашықтан басқару мүмкіндігі болуы мүмкін).

Linux арналған Firewall. Linux ОЖ арналған қауіпсіздік сұрақтары өте басым болып табылады, және сол үшін Firewall ОЖ өзегінің деңгейінде кіріктірілген және IP Firewall деп аталады. Болашақта Firewall әрекет ету қағидаларын соның мысалында қарастырады. Алайда одан бөлек осында қысқаша қарастыратын желіаралық экрандардың бірнеше жүзеге асырылуы бар.

Ережеге сәйкес, мұнда әңгіме басқа ОЖ секілді арнайы бағдарламалық құралдар туралы айтылып отырған жоқ, әңгіме желілік қауіпсіздік сұрақтарын шешуге ғана арналған мамандандырылған дистрибутивтер туралы айтылып отыр. Ережеге сәйкес мұндай шешімдердің кішкене мөлшері болады, орнату мен баптауда қарапайым және түсінікті, ал қолда бар функциялар үй/ұжымдық желіні желілік шабуылдар мен вирустардан қорғай отырып, Интернетке қосуға мүмкіндік береді. Қосымша олардың көбісінде трафикті бақылау, протоколдарды бұғаттау, антиспам сүзгі және көптеген басқа функцияларға ие болады.

Linux кіріктірілген Firewall басқа тағы арнайы әзірлеген Firewall қатарын қарастырайық.

Untangle Gateway. Untangle компаниясы шығарады, Интернетке қауіпсіз қолжетімділікті қамтамасыз ете отырып, коммерциялық шешімдерді алмастыра алады. 50-300 және одан көп кішкентай және орта ұйымдарға (жүйелік талаптар 50 үшін келтірілген) қарастырылған. Untangle негізі Debian болып табылады, барлық баптаулар түсінікті, бірақ шектелмеген интерфейстің көмегімен жүргізіледі. Бақсару үшін мәнін түсінудің өзі жеткілікті, қарапайым жағдайда UNIX-жүйелердегі терең білім талап етілмейді. Web-технологияларды қолданатын басқа шешімдермен салыстырғанда Untangle интерфейсі Java-да жазылған, сол үшін басқару консоліндегі барлық өзгерістер, жұмыс істеу статистикасы нақты уақытта шығарылады, бұл Java қолданған үшін жоғары жүйелік талаптар арқылы төлеу қажет болғанына қарамастан өте ыңғайлы болып табылады.

Untangle конструктор түрінде орындалған. Базалық жүйені орнатқаннан кейін онда қорғаныс модульдері болмайды, әкімші міндеттерге және қолда бар қондырғыға байланысты шындығында керек нәрсені өз бетінше таңдайды. Untangle келесілерді қамтамасыз ететін 94 пакетті (19 қосымшаны) қосуға болады: бағдарлауды, антивирустық/антифишинг/spyware қорғанысты, шабуылдарды анықтауды, протоколдарды талдауды, Web-трафикті контенттік сүзгілеуді, VPN-қосылуды және көптеген басқа функцияларды. Кейбір төмен деңгейлі желілік шабуылдардан тегін берілетін «Attack Blocker» өзіндік дайындалған модулі қорғайды. Қажет болған жағдайда протоколдарды талдау модулі стандартты емес

порттарды қолданғанына қарамастан қолданбалы деңгейлі кез-келген протоколдардың жұмысын шектеуге қабілетті.

Endian Firewall Community. Endian Firewall (EFW) негізі блып бастапқы уақыттан бастап әзірлеушілер интерфейс қауіпсіздігі мен ыңғайлылығының функцияларын күшейтуді шешкен IPCop Firewall қызмет етті. EFW CentOS негізінде тұрғызылады және сыртқы қауіп-қатерден қорғау құралдарының толық жинағын қамтиды, бұл оны UTM-жүйелерге (Unified Threat Management) жатқызуға мүмкіндік береді. Бұл пакеттік сүзгі (netfilter), контент сүзгісі, HTTP/FTP/POP3/SMTP трафигін антивирустық тексеру, спамнан қорғау, антиспуфинг және антифишинг модульдері. Сүзгілеу және бағдарлау саясаттары барлық дерлік өзекті ақпаратты көрсетуге мүмкіндік береді — протокол, порт, желілік интерфейс, IP- және MAC-мекенжайлар. Контенттік сүзгіде 20-дан астам категориялар мен кіші категориялардың дайын баптаулары болады.

Интерке қосылу Ethernet, PPPoE, ADSL (USB, PCI), ISDN, модемнің, соның ішінде 3G арқылы жүзеге асырылған. Сыртқы интерфейске бірнеше IP-мекенжайларды тағайындауға болады. Пайдаланушыларды жергілікті сәйкестендіруден бөлек Active Directory, LDAP және RADIUS қолдауы қарастырылған. EFW құрамында қорғалған VPN қосылысты ұйымдастыруға арналған екі қосымша бар: OpenVPN және Openswan/Pluto. Қосылыстар, трафик, пайдаланушылардың жұмысы бойынша статистика жүргізіледі. Белгілі бір оқиғалар орын алған кезде әкімшінің e-mail хабарлама жіберіледі.

IPCop Firewall. SOHO (Small Office, Home Office) дистрибутиві — кіші және үй кеңсесі нарығына бағытталған, сол үшін әзірлеушілердің басты міндеті интерфейсті ыңғайлы және қарапайым ету болып табылады. Жеткізілімде қорғалған шлюзді ұйымдастыру үшін қажеттінің барлығы болады — пакеттер сүзгісі, IDS/IPS, прокси-серверлер, Web-сервер, DNS, DHCP сервер/клиенті, Openswan, OpenVPN, трафикті шектеу, NTP-сервер. IP-мекенжайлар және жүйе атауы бойынша Web-прокси арқылы қосылыстарды бақылау жүзеге асырылған.

Базалық жеткізілімді жетпейтіннің барлығы шеттегі бағдарламалаушылар әзірлейтін және қолдайтын қосымшаларда қолжетімді. Олардың ішінде URL сүзгісі, Firewall ілгері баптаулары, Web және SMTP трафиктердегі вирустар мен көптеген басқаларды тексеру кіреді. Сыртқы интерфейс Ethernet (статикалық, DHCP), PPTP, PPPoE, ISDN бойынша, сонымен бірге модемдік қосылу арқылы қосылуды қолдайды. Кейбір операцияларды (қосылу, өшіру, жаңарту және т.б.) кесте бойынша орындауға болады.

Орнату процессі жалған графикалық консольде жүргізіледі және өте қарапайым. Басқару консолі де өте қарапайым.

SmoothWall Express. 2000 ж. ортасында пайда болған жоба ескірген компьютерді баптауларымен қарапайым қолданушы жұмыс істей алатын қорғаныс функциялары бар толыққанды шлюзге айналдыруды өз алдына мақсат етіп қойған болатын. SmoothWall құрамында қажеттінің барлығы бар — Firewall, порттардың форвардингі, VPN қолдау, прокси-серверлер, Web-сервер, дайын сүзгілері және трафикті журналдары бар DNS, DHCP-сервер, NTP, QoS қолдау. Тәулік уақытына байланысты белгілі бір мекенжайлар үшін Интернетке шығу қолжетімділігін орнату ықтимал. Қажет болған жағдайда трафик Clamav антивирусының көмегімен тексеріледі. Алдыңғы екі дистрибутивтерде секілді төрт желілік қосылыстарға дейін қуатталады: WAN, LAN, DMZ, Wi-Fi.

Оның орнатылымы өте қарапайым: бірнеше рет ОК басу жеткілікті, және процедура аяқталды. Ары қарай бастапқы баптаулар жүреді — тарату, hostname және шығыс трафик саясатын таңдау:

- Open — жалпы шығыс трафик рұқсат етілген;
- Half-Open — тек негізгі порттар бойынша ғана қосылуға рұқсат етілген, потенциал қауіпті қосылыстар бұғатталған;
- Closed — барлық шығысы қосылыстар бұғатталған.

Одан кейін желі типі бапталады. Интерфейстер мен қосылыстардың типтері ұсынылады. Осыдан кейін тағайындалуы бойынша желілік құрылғылар үлестіріледі, интерфейс, шлюз және DNS-сервердің мекенжайлары көрсетіледі.

Vyatta. Vyatta дистрибутивін әзірлеушілер Cisco Systems бәсекелестік етуге шешім қабылдады. Негіз ретінде Debian ала отырып, олар оны әзірлемесімен *Intel* және *Microsoft* алыптардың қаржыландыруымен ICSI (International Computer Science Institute)Беркли тобы айналысатын XORP (eXtensible Open Router Platform, xorp.org) бағдарлаудың еркін таратылатын платформасымен біріктірді. Vyatta-компьютерді орната отырып, прокси мен URL (Squid + SquidGuard) сүзгісін, (Network Access Policies) желілік амалдарды, OpenVPN, DNS Forwarding, Ethernet Bonding және Bridget Ethernet over ADSL (RFC 2684) кэштейтін IDS/IPS функциялары бар маршрутизаторды аламыз.(T1/E1, T3 және т.б.) мультипортты карталар мен сымсыз 3G-модемдерін қолдайды.

Vyatta алғашқы нұсқалары Cisco маршрутизаторлары секілді командалық жол арқылы бапталатын. Одан кейін Web- интерфейс қолжетімді болды. Қазіргі күні өте танымал виртуал машиналар — VMware, Xen, Hyper-V және кейбір басқа гипервизорлардың ерекше қолдауы ерекшеленеді. Дистрибутив баптауларды флэш немесе басқа тасымалдаушыға (config.boot файлы) сақтаумен LiveCD бірге жұмыс істей алады. Хард, USB-салпыншақ немесе Compact Flash картасына орнату ықтимал. Екі диск бар болған жағдайда орнатушы оларды RAID 1 автоматты түрде байланыстыруға мүмкіндік береді.

Орнату процессі командалық жол көмегімен жүргізілетіндігіне қарамастан, өте қарапайым. *Vyatta* құпиясөзімен *root* ретінде тіркелейік және инсталляторды іске қосайық:

```
#install-system
```

Ары қарай орнатуды растаймыз және бөлімдерді қалыптастыруға кірісеміз. Үнсіз келісім бойынша *Auto* тұрады. «Yes» енгізу арқылы дисктегі мәліметтерді жоюды растаймыз, түбірлі бөлім мөлшерін (үнсіз келісім бойынша барлық диск) көрсетеміз және мәліметтер көшірілгенге дейін күтеміз. Одан кейін *Root* және *vyatta* пайдаланушылардың құпиясөздерін орнатамыз, осыдан кейін қайта жүктейміз және конфигурациялау режиміне өтеміз:

```
# configure
```

Желілік интерфейсті баптаймыз:

```
# set interfaces ethernet eth0 address 192.168.1.1/24
# set interfaces ethernet eth0 description LAN
```

Осыдан кейін Web-интерфейсті қосуға болады:

```
# set service https
```

Осыған ұқсас басқа қызметтер де қосылады — nat, dns, dhcp- relay, dhcp-server, webproxy, ssh.

Барлық орнатылымдарды растаймыз:

```
# commit
```

Енді келесі команданы пайдалана отырып, не орын алғандығын көруге болады:

```
# show interfaces
```

Show-all теру арқылы барлық баптауларды шығаруға болады. *Exit* командасы бойынша редакциялау режимінен шығамыз. Ары қарай баптауды Web-интерфейсті қолдану арқылы орындауға болады. Қажетті категорияны таңдаймыз және *Create*

батырмасын басамыз, осыдан кейін ұсынылған өрістерді толтырамыз. Жоғарыдағы *Show* батырмасы «+» белгісімен қосылған, бірақ әлі белсендірілмеген параметрлер жарықтандырылатын конфигурациялық файлды көрсетеді. Оларды іске қосу үшін *Commit* (бас тарту — *Discard)* батырмасын басамыз.

2.5. LINUX TCP/IP FIREWALL

Linux үшін айрықша болатын техникалық мәселелер мен әдістерге бағытталатын боламыз. Берілген Firewall егжей-тегжейлі зерттеудің алдында зиянкестердің әрекеттерінен желіде бізді атыстыратын кем дегенде ең көп таралған қауіп-қатерді толығырақ қарастырған жөн. Біз қорғайтын желіге шабуылдайтын әсер әдістері бойынша олардың қарапайым классификациясын келтіреміз. Желілік әкімшінің компьютерлік қорғанысқа потенциал шабуылдардың сипатын түсінуі маңызды. Linux IP Firewall нақты неге қарсы қорғайтындығын, ал нақты неге қарсы қорғамайтындығын жақсырақ түсінуге болатындай шабуылдардың ең маңызды типтерін қысқаша сипаттайық. Шабуылдың негізгі жолдары үшін стандартты қорғау әдістері бар, олар туралы сөз кейінірек айтылатын болады.

Рұқсат етілген қол жеткізу. Бұл қорғалатын жүйелерге бұл істі жасамаған жөн болатын адамның қосылып жатқандығын білдіреді. Мысалы, біреу NFS тізімдемелерін жөндеуге талпынып жатыр.

Бұ шабуылды болдырмаудың әр түрлі тәсілдері бар. Осы қызметтер арқылы қолжетімділікті кімнің ала алатындығын мұқият анықтай отырып, рұқсат етілген пайдаланушылардан бөлек барлық адамдардың желілік қолжетімділігінің алдын алуға болады.

Бағдарламалардағы таныс әлсіздікті эксплуатациялау. Кейбір бағдарламалар мен желілік қызметтер бастапқы ата күшті қорғаныспен әзірленген жоқ болатын. Мұның мысалы: BSD remote services (rlogin, rexec және басқа r-қызметтер). «Эксплойт» термині дәл осы шабуылдар түрінен пайда болған болатын. Осы шабуыл типіне қарсы өзіңді қорғаудың ең жақсы тәсілі кез-келген осал қызметтерді өшіру немесе мұндай қателіктер түзетілген олардың ең соңғы нұсқаларын іздеп көру болып табылады.

Denial of service. Denial of service attacks (қызмет көрсетуді мойындамау шабуылдары) деп аталатындар қызмет немесе бағдарламаның жұмыс істемеуіне мәжбүрлейді немесе басқаларға оларды қолдануға мүмкіндік бермейді. Олар қызмет жұмыс істей алмайтын мұқият дайындалған пакеттер жіберілімімен желілік деңгейде орындалуы мүмкін. Сонымен бірге олар мұқият дайындалған командалар таңдалған қызметті қайта жүктеуге міндетті болатын қолданбалы бағдарлама деңгейінде орындалуы мүмкін.

Күдікті желілік трафик пен бағдарламалардың күдікті командаларын жою — мұндай шабуылдардың тәуекелін азайтудың ең жақсы жолдары болып табылады. Шабуылдау әдісінің егжей-тегжейін білу пайдалы, сол үшін осы облыстағы жаңа әзірлемелерді зерттеу қажет. Хакерлік бағдарлы сайттар дәл осы себепке байланысты желілер әкімшілерінің арасында өте танымал.

Spoofing. Шабуылдың бұл типі компьютер немесе қолданбалы бағдарламаны одан күтілетін емес, басқаша жұмыс істеуге мәжбүрлейді. Мысалы, көптеген қорғаныстарда IP-мекенжай бойынша тексеру қолданылады. Жаудың компьютері өзін дұрыс мекенжайлы машина ретінде ұсынуы әбден мүмкін, бұл одан пакеттердің шабуылданатын жүйеге еніп кетуіне мүмкіндік береді. Мысалы, BSD

rlogin қызметіне арналған танымал эксплойт осы тактиканы жақсы қолданады.

Осы шабуылдар типіне қарсы қорғаны қарапайым: шындығында пакеттің қайдан келгендігін және ішкі ақпараттың оған қосылатын ортаға сәйкестігін мұқият қадағалау керек.

Eavesdropping. Бұл шабуылдың ең қарапайым типі. Қандай да бір компьютер оған тиесілі емес мәліметтерді «тыңдайтындай» және жинайтындай конфигурацияланған. Сауатты жазылған тыңшы жүйеге кіру үшін пайдаланушы аты мен оның құпиясөзіне ие болуы мүмкін. Тарату ауқымы кең желілер, мысалы Ethernet осы шабуылға көп шалдыққыш болып келеді, себебі олардағы барлық пакеттер желідегі барлық машиналар арқылы өтеді, ал оған қажетті пакеттердің таңдауымен әрбір нақты машина айналысады. Мұнда трафикті шифрлеу көмектеседі.

Айтылған шабуылдарды көрсетудегі IP Firewall орны. IP Firewall рұқсат етілмеген қол жеткізу, қызмет көрсетуді мойындамау шабуылдарының және IP Spoofing алдын алу немесе төмендетуде өте тиімді. Ол желілік қызметтер немесе бағдарламаларда әлсіздіктерді эксплуатациялаудан кету кезінде, сонымен бірге білдірмей тыңдаудан қорғау кезінде аса тиімді емес.

IP Firewall. Firewall түсінігінің Linux нақты жүзеге асырылуына қатысты түсіндірмесін қарастырайық. Firewall — бұл ұйым ішкі желісі мен сыртқы желісінің арасында орналасқан машинада жұмыс істейтін бағдарлама. Жалпы жағдайда мұндай желі Интернет болып табылады, бірақ бұл міндетті емес.

Firewall пакеттермен алмасу протоколдарының деңгейінде желілік трафигін сүзгілеуді орындайды. Ол белгілі бір критерийлерге жауап беретін пакеттерді сыртқы желіден ішкі желіге өткізеді, және керісінше. Критерийлер өте күрделі болуы мүмкін сүзгілеу ережелері арқылы қойылады. Пакеттер сүзгісі берілген критерийлерге сәйкес келмейтін пакеттерді де серпиді. Бұл ретте машина-ашқышқа қателік туралы хабарлама жіберілуі мүмкін (мүмкін жіберілмеуі де мүмкін, баптауға байланысты).

Осылайша, Firewall желіні ішкі ұйымдастыруды сыртқы әлемнен жасырады және оның жұмысының сенімділігін арттырады. Желі хакерлердің шабуылдарынан қорғалған болады. Өкінішке орай, мұндай тәсілдеме толық қорғанысқа кепілдік бермейді: әрқашан Firewall айналып өтуге қабілетті ақылды хакер табылады. Бірақ сонда да Firewall хакерлердің өмірін бірден қиындатады.

Linux өзегі IP Firewall кіріктірілген функцияларын ұсынады. Өзектің желілік коды желілік сүзгілеуді (IP Filtering) бірнеше тәсілдермен жүзеге асырады және сүзгілеу ережелерін басқару үшін арналған интерфейсті ұсынады. Бұдан бөлек, Linux Firewall тікелей пакеттерді сүзгілеумен байланысты болмайтын тағы екі тиімді функцияларға ие болады. Бұл IP Accounting және IP Masquerade.

IP Filtering. Бұл қандай IP-пакеттердің өңделетіндігін, ал қандайларының шығарылатындығын шешетін қарапайым механизм. «Шығарылған» терминді пакеттің жойылатындығын және ешқашан болмаған секілді еленбейтін болатындығын білдіреді. Қандай пакеттерді сүзгілеу керектігін анықтау үшін көптеген әр түрлі критерийлерді қолдануға болады. Міне олардың кейбірі.

1. Протоколдар типтері: TCP, UDP, ICMP және т.б.

TCP (Transmission Control Protocol — таратуды басқару протоколы) — TCP/IP желілері мен кіші желілерінде мәліметтерді таратуды басқаруға арналған Интернет мәліметтерін таратудың негізгі протоколдарының бірі. IP протоколдарының стегіндегі машиналық деңгей протоколының функцияларын атқарады. TCP механизмі қосылысты алдын ала орнатуы бар мәліметтердің ағынын ұсынады, мәліметтерден айырылу жағдайында мәліметтерді қайталап сұратуды жүзеге

асырады және UDP салыстырғанда таратылатын мәліметтердің бүтіндігіне және тарату нәтижесі туралы жіберушінің хабарламасына кепілдік беретін бір пакеттің екі көшірмесін алған кездегі қайталауды болдырмайды.

UDP (User Datagram Protocol — пайдаланушылық датаграмм протоколы) — Transmission Control Protocol/Internet Protocol, Интернетке арналған желілік протоколдар жинағының басты элементтерінің бірі. UDP бірге компьютерлік қосымшалар арнайы тарату арналарын немесе мәліметтер жолдарын орнату үшін алдын ала хабарлау қажеттілігінсіз IP-желі бойынша басқа хосттарға хабарламаларды (бұл жағдайда датаграммалар деп аталатын) жібере алады. UDP мәліметтердің сенімділігін қамтамасыз ету, бірыңғайландыру немесе бүтіндігін қамтамасыз ету үшін анық емес «амандасусыз» таратудың қарапайым моделін қолданады. Осылайша, UDP сенімсіз қызметті ұсынады, және датаграммалар тәртіпсіз келуі, қайталануы немесе ізсіз мүлдем жоқ болып кетуі мүмкін. UDP қателіктерді тексеру мен түзету не керек емес, не болмаса қосымшада орындалуы тиіс дегенді білдіреді. Уақытқа сезімтал қосымшалар жиі UDP қолданады, себебі нақты уақыт жүйелерінде мүмкін емес болуы мүмкін кешіктірілген пакеттерді күтуден гөрі пакеттерді шығарып тастау дұрысырақ болады. Интерфейстің желілік деңгейінде қателіктерді түзету қажет болған жағдайда қосымша осы мақсатта әзірленген TCP немесе SCTP әрекет етуі мүмкін.

ICMP (Internet Control Message Protocol — желіаралық басқарушы хабарламалар протоколы) — TCP/IP протоколдарының стегіне кіретін желілік протокол. Негізінен ICMP қателіктер мен мәліметтерді тарату кезінде орын алған басқа да айрықша жағдайлар туралы, мысалы, сұратылып жатқан қызмет қолжетімді емес, немесе хост немесе маршрутизатордың жауап бермейтіндігі туралы хабарламаларды тарату үшін қолданылады. Сонымен бірге ICMP кейбір қызметтік функциялар жүктеледі.

TCP/IP протоколдарының стегіне бірнеше протоколдар қатары кіреді, олардың ішінде *SCTP* (Stream Control Transmission Protocol — ағынды басқаруы бар тарату протоколы) — компьютерлік желілердегі машиналы деңгейдің салыстырмалы түрде жаңа протоколы, DCCP (Datagram Congestion Control Protocol) — IETF әзірлейтін OSI моделінің машиналық деңгейінің протоколы, 2006 ж. наурызында стандарт ретінде қабылданған, қолданбалы деңгейде қалыптастыру қажеттілігін болдырмай желідегі артық тиеуді қадағалау үшін арналған механизмдерді ұсынады, қажетті тәртіпте ақпаратты жеткізуге кепілдік бермейді; *IGMP* (Internet Group Management Protocol — Интернет топтарын басқару протоколы) — IP протоколына негізделген желілердегі мәліметтерді топтық таратуды бақсару протоколы (multicast). IGMP маршрутизаторлар және IP-түйіндер желілік құрылғыларды топтарға ұйымдастыру үшін қолданады.

2. Порттардың нөмірлері (бұл TCP/UPD секілді мәліметтерді тарату протоколдарына қатысты).
3. Пакет типтері: SYN/ACK, data, ICMP Echo Request және т.б.
4. Пакет келген желілік мекенжай.
5. Пакет жіберілген желілік мекенжай.

IP-сүзгілеу — желілік деңгей құралы, бұл ретте ол желілік қосылыстарды қолданатын қолданбалы бағдарламаға қатысты ешнәрсені түсінбейді, бірақ тек тікелей қосылыстарға ғана қатыстыны түсінеді.

Мысалы, telnet-порт арқылы қорғалатын ішкі желіге пайдаланушылардың қолжетімділігін қабыл алмауға болады, алайда егер тек IP-сүзгілеуге ғана сүйенетін болса, Firewall арқылы пакеттерді таратуға рұқсат етілген портпен telnet бағдарламасын қолдануға тиым салуға болмайды. Firewall арқылы өтетін әрбір

қызмет үшін арналған прокси-серверді қолдана отырып, осы мәселелердің алдын алуға болады. Прокси-серверлер олар әзірленген қолданбалы бағдарламаны түсінеді, және Firewall порт арқылы World Wide Web үшін айналып өту үшін telnet бағдарламасын қолдану типін теріс пайдалануға жол бермейді. Егер Firewall World Wide Web арналған проксиді қолдайтын болса, telnet тек онымен бірге ғана қосылатын болады және тек HTTP-сұраныстар ғана өтетін болады. Прокси-серверлердің коммерциялық та, бос та көптеген мөлшері бар.

IP-сүзгілеу ережелерінің жинағы көптеген ережелерді қояды. Ең қарапайым жағдай мысалында қарастырайық. Айталық, Our College network желісіндегі World Wide Web пайдаланушыларына Интернеттегі тек басқа Web-серверлерге ғана жүгінуге мүмкіндік беру қажет. Ол үшін Firewall келесі пакеттерді өткізуге баптау талап етіледі:

1) Our College network желісінің бастапқы мекенжайларымен кез-келген тағайындалған сайттар мен 80 (WWW)порттарға;
2) Our College network желісіндегі тағайындау мекенжайымен және 80 (WWW) тағайындау портымен кез-келген бастапқы мекенжаймен.

Мысалда сүзгілеудің екі ережесі қолданылған. Міндетті сәтті шешу үшін мәліметтердің Our College network желісінен шығуға мүмкіндік беру керек, сонымен бірге сұраныстарға жауаптарды қайтаруға мүмкіндік беру керек. Linux мұны қысқартады және бұл ережелерді бір командада анықтау мүмкіндігін береді.

2.6. LINUX IP FIREWALL ОРНАТУ ЖӘНЕ ІСКЕ ҚОСУ

Linux IP Firewall Linux ОЖ қорғанысының кіріктірілген функциясы болып табылады, сәйкесінше, оны бөлек орнату талап етілмейді. Таралған дистрибутивтердің көбісінде ол автоматты түрде орнату кезінде орнатылатын бағдарламалық қамсыздандырудың құрамына кіреді және тек баптауды талап етеді. Алайда егер ол орнатылмаған болса, онда келесі ұсыныстарға назар аударған жөн.

Linux IP Firewall іске қосу үшін IP Firewall қолдайтын өзек пен сәйкес конфигурациялық утилиталар бапталған болуы тиіс. 2.2-серияға дейінгі өзектерде *ipfwadm* утилитасын қолдану керек. 2.2.x өзектерінде Linux арналған IP Chains деп аталатын IP Firewall үшінші буыны болады. IP Chains *ipchains* бағдарламасын қолданады. Linux 2.3.15 және одан жоғары өзектер Linux IP Firewall төртінші буыны – netfilter қолдайды. Netfilter пакетінің коды — пакеттерді Linux өңдеу ағынының үлкен өзгерістерінің нәтижесі, бұл ретте netfilter ipfwadm және ipchains бірге кері үйлесімділікті қамтамасыз етеді. Бұл нұсқа *iptables* командасы арқылы бапталады. Ары қарай осы өсірімдердің ерекшеліктері толығырақ қарастырылатын болады.

Linux өзегін IP Firewall қолдауға баптау қажет. Ол үшін өзекті баптау кезінде, мысалы, *make menuconfig* командасы арқылы тек параметрлерді көрсету қажет. 2.2 өзектерінде келесі опцияларды таңдау талап етіледі:

```
Networking options ---------------- >
    [*] Network firewalls
    [*] TCP/IP networking
    [*] IP:          firewalling
    [*] IP:          firewall packet logging
```

2.4.0 және жоғары сериялы өзектерде көбірек опцияны таңдаған жөн:

```
Networking options ----------------- >
    [*]     Network packet filtering (replaces ipchains)
      IP:   Netfilter Configuration ------------------->
    <M>     Userspace queueing via NETLINK
    (EXPERIMENTAL)
    <M>     IP tables support (required for filtering/
    masq/NAT)
        <M> limit match support
        <M> MAC address match support
        <M> netfilter MARK match support
        <M> Multiple port match support
        <M> TOS match support
        <M> Connection state match support
        <M> Unclean match support (EXPERIMENTAL)
        <M> Owner match support (EXPERIMENTAL)
        <M> Packet filtering
        <M> REJECT target support
        <M> MIRROR target support (EXPERIMENTAL)
        <M> Packet mangling
        <M> TOS target support
        <M> MARK target support
        <M> LOG target support
        <M> ipchains (2.2-style) support
        <M> ipfwadm (2.0-style) support
```

2.7. КЕСТЕЛЕР МЕН ТІЗБЕКТЕРДІҢ ӨТУ ТӘРТІБІ

Тәжірибеде өте жиі кездесетін типтік шешімдерді шешу үшін арналған ережелерді қалай әзірлеуге болатындығын қарастырайық. Ол үшін алдымен сүзгілеуді басқару үшін арналған негізгі құралдарға қысқаша шолу жасайық.

Ipfwadm **утилитасы**. ***Ipfwadm*** (IP Firewall Administration) утилитасы 2.2.0 нұсқасына дейінгі өзектерде ережелерді басқару үшін қажет. Оның синтаксисі өте күрделі, бірақ ол бірнеше аса қарапайым мысалдарда қарастырылатын болады.

Ipfwadm утилитасы барлық заманауи Linux дистрибутивтерде бар, бірақ, бәлкім, үнсіз келісім бойынша қойылмайды. Бөлек қою қажет болатын арнайы желілік пакет болуы мүмкін.

Ipchains **утилитасы**. ***Ipfwadm*** **секілді** ***ipchains*** **утилитасы, бірінші көзқарасқа, оған дағдыланғанға дейін естен шығаруы мүмкін**. Ол қысқартылған синтаксисі бар ***ipfwadm*** икемділік утилиталарын қамтамасыз етеді және көптеген ережелерді басқаруға және оларды бір-бірімен байланыстыруға мүмкіндік беретін жинақтар немесе тізбектердің механизмін (chaining) қосымша қамтамасыз етеді. Кешірек ережелер тізбегін әзірлеу қарастырылатын болады.

Ipchains **командасы** Linux дистрибутивтерінде, 2.2 сериялы өзектерде пайда болды. Бұл пакетке ***ipchains*** мүмкіндіктерін қолдана отырып, ipfwadm жұмысына ұқсататын ***ipfwadm-wrapper*** скрипті кіреді. Бұл Firewall жаңа нұсқасына бейімделуді айтарлықтай қысқартады.

Iptables **утилитасы**. ***Iptables*** **синтаксисі** ***ipchains*** **синтаксисіне өте ұқсас**. Кеңейтілімдер модульдерін қолдауда және пакеттерді сүзгілеудегі жаңалықтар

қатарында айырмашылық бар.

***Iptables* утилитасы *netfilter* пакетіне кіреді**. Сонымен бірге ол 2.4 және одан жоғары өзекте Linux дистрибутивтеріне кіреді.

Сүзгілеудің үш тәсілі. IP-пакеттерді бағдарлаумен айналысатын машинамен өңдеудің жалпы қағидасын түсіну үшін бағдарлау процессінде орын алатын негізгі оқиғаларды қарастырайық, және оларға келесі бірегей нөмірлерді берейік.

(1) IP-пакет бір жерден келді және оның осы машинадағы процесс үшін арналған ба екендігін анықтау үшін зерттелетін болады.

(2) Егер келген пакет осы машинаға арналған болса, онда ол сол машинада өңделетін болады.

(3) Егер пакет ол машинаға арналмаған болса, онда сәйкес бағдар үшін бағдарлау кестесі бойынша іздеу орындалатын болады, және пакет сәйкес интерфейске жіберіледі немесе егер бағдар табылмайтын болса, өткізілетін болады.

(4) Жергілікті процесстердің пакеттері сәйкес интерфейске жіберу үшін бағдарлауды бағдарламалық қамсыздандыруға жіберілетін болады. Шығыс IP-пакет ол үшін өзекті бағдардың бар ма екендігін анықтау үшін зерттелетін болады; егер ондай болмайтын болса, онда ол өткізілетін болады.

(5) IP-пакет бір жаққа жіберіледі.

Енді желідегі пакеттер ағынының қалай әзірленетіндігін талдайық.

1. Бұл сұлбада (1)—(3)—(5) ағыны Ethernet желісіндегі компьютер арасындағы мәліметтерді қандай да бір байланыс арқылы басқа қолжетімді компьютерге бағыттайтын біздің машинамызды білдіреді. Алдымыздағы мысалдарда бұл PPP болады.

PPP (Point-to-Point Protocol) — OSI желілік моделінің арналық деңгейлі екі таңбалы протоколы. Әдетте желінің екі түйіндері арасындағы тікелей байланысты орнату үшін қолданылады, әрі ол қосылысты сәйкестендіру, шифрлеу мен мәліметтерді қысуды қамтамасыз етуі мүмкін. Физикалық желілердің көптеген типтерінде қолданылады: нөл-модемдік кабель, телефон линиясы, ұялы байланыс және т.б. Ethernet арқылы, және кейде DSL арқылы қосылу үшін қолданылатын Point-to-Point Protocol over Ethernet (PPPoE); DSL үшін PPPoE негізгі баламасы болып табылатын ATM Adaptation Layer 5 (AAL5) бойынша қосылу үшін қолданылатын Point-to-Point Protocol over ATM (PPPoA) секілді PPP протоколының түршелері жиі кездеседі.

2. (1)—(2) және (4)—(5) ағындары мәліметтерді енгізуді және біздің жергілік компьютерде жұмыс істейтін желілік бағдарламаның шығыс ағындарын көрсетеді.

3. (4)—(3)—(2) ағыны сақиналы ішкі интерфейс бойынша (loopback connection) мәліметтерді таратуды білдіреді.

Linux өзегінің IP Firewall бұл процесстегі әр түрлі сатыларда сүзгілеуді қолдана алады, яғни келесідей IP-пакеттерді сүзгілей алады:

- біздің машинаға келеді;
- оның ішінде жүреді;
- сыртқы әлемге жіберуге арналған.

Пакеттерді сүзгілеу келіп түсетін пакеттерге қатысты қолданылатын ережелерді әзірлеуге негізделген. Пакетке қатысты ережелерді қолдану нәтижесі үш әрекеттің біреуі болады: рұқсат ету, тиым салу немесе қайта жіберу.

Сүзгіге арналған ережелерді жазу тәртібі өте маңызды, себебі дәл осы тәртіпте пакеттер талданатын болады.

Пакеттің қозғалыс бағытына байланысты ережелер категорияларға бөлінеді:

- *Input* — кіріс пакеттерге арналған;
- *Output* — шығыс пакеттерге арналған;
- *Forwarding* — компьютер арқылы өтетін транзитті пакеттерге арналған.

Ipfwadm және *ipchains Input* ережесі (1) ағынына қатысты қолданылады, *Forwarding* ережесі — (3) ағынына және *Output* ережесі — (5) ағынына қатысты қолданылады. Кейінірек, netfilter талқылаған кезде біз *Input* ережесінің ағында қолданылатындай және *Output* ережесінің (4) ағынында қолданылатындай қандай ұстап қалу нүктелерінің өзгергендігін көреміз. Бұл ережелер жинағының қалай құрылымдалуы үшін үлкен мәнге ие, бірақ ортақ қағида Linux Firewall барлық нұсқалары үшін сенімді болып қалады. Бұл алдымен аса күрделі болып көрінуі мүмкін, алайда ессесіне күрделі және күшті конфигурацияларды әзірлеуге мүмкіндік беретін икемділікті қамтамасыз етуге мүмкіндік береді.

***Ipfwadm* қолдану**. *Ipfwadm* командасы Linux IP Firewall екінші буынына арналған конфигурациялау құралы болып табылады. Ipfwadm командасын қолдануды сипаттаудың ең қарапайым тәсілі — мысалдар.

Айталық, Интернетпен байланысу үшін Firewall бар Linux-машинасын қолданатын кішкене ұйым желісі бар. Осы желінің пайдаланушыларына Интернеттегі Web-серверлерге жүгінуге рұқсат береміз, бірақ қандай да бір басқа трафикке жол бермейміз. Ол үшін біздің желідегі бастапқы мекенжайы және 80 тағайындау порты бар пакеттерді сыртқа жіберу ережелерін анықтау, сонымен бірге жауаптары бар пакеттерді алу талап етіледі.

Айталық, Желіде 24 битті желілік маска (С классы) болады және оның желілік мекенжайы 172.16.1.0. Әрбір ереже *ipfwadm* утилитасының көмегімен командалық жолда бөлек командамен беріледі. Біздің мысалға арналған ережелер келесі жолмен берілетін болады:

```
#    ipfwadm -F -f
#    ipfwadm -F -p deny
#     ipfwadm -F -a accept -P tcp -S 172.16.1.0/24 -D 0/0 80
#     ipfwadm -F -a accept -P tcp -S 0/0 80 -D 172.16.1.0/24
```

- Мұнда «#» таңбасы командалық жолдың басында команданың супер пайдаланушының (root) атынан орындалуы тиіс екендігін білдіреді. Енді нақты командаларды қарастырайық.
- Барлық төрт командада болатын F параметрі *ipfwadm* көрсетеді және пакеттерді жіберу ережесі анықталады (forwarding), яғни ереже Firewall орнатылған компьютер арқылы транзитпен өтетін пакеттер үшін әрекет етеді.
- Ipfwadm бірінші командасы транзитті пакеттерге арналған барлық ережелерді тазартуды тағайындайды. Ережелер ережелер жинағының «ұшына» қосылатындықтан, бұл біздің мәлім жағдаймен жұмыс істейтінімізге кепілдік береді, және ережелерді қосқаннан кейін қандай да бір тағы мәлім емес ережелердің қалғандығы табылмайды.
- Екінші ереже үнсіз келісім бойынша берілген жіберу стратегиясын орнатады. Өзектің біз кейінірек рұқсат беретін барлық IP-пакеттерді жіберуден бас тартуы керек екендігін хабарлаймыз. Бұл өте маңызды сәт, себебі мұнда қандай да бір ережеге сәйкес келмейтін барлық пакеттердің тағдыры анықталады.
- Үшінші және төртінші ережелер өткізілетін пакеттерге талаптарды анықтайды. Үшінші команда біздің пакеттерге жүйеден сыртқа шығуға мүмкіндік береді, ал төртінші ереже жауаптардың келуіне мүмкіндік береді.

Сүзгілеу ережелерін сипаттаған кезде келесі параметрлер қолданылды:

- *—F* — жіберу ережесін анықтайды *(Forwarding),* соған сәйкес әрекет тек

транзитті пакеттерге қатысты ғана таралады;

- —*a* (accept — қабылдау) — осы ережеге сәйкес келетін барлық пакеттерді қабылдауға мүмкіндік беретін accept стратегиясы бар ережені қосады;
- —*P tcp* — ереже тек TCP-пакеттерге ғана қатысты қолданылады (UDP немесе ICMP пакеттеріне тиіспейді);
- *-S 172.16.1.0/24* — шығы мекенжайда *(Source)* 24 бит кіші желісінің маскассы болуы керек және желі мекенжайы 172.16.1.0 болуы тиіс;
- — *D 0/0 80* — тағайндалу мекенжайында *(Destination)* (0.0.0.0) нөлдік биттері болуы тиіс. Бұл желідегі кез-келген мекенжайға сәйкес келеді. 80 саны тағайындау портын анықтайды, бұл жағдайда WWW. Желілік қызметтер мен порттар атауларының сәйкестіктерін көрсетілген */etc/services* файлынан кез-келген жазбаны қолдануға болады, мысалы,*D 0/0* www портын анықтау үшін.

Ipfwadm утилитасы желілік маскаларды салыстырмалы түрде сирек қолданылатын форматта қабылдайды. Ондағы */nn* жазбасы масканың мөлшері қанша битті қамтитындығын білдіреді. Биттер сол жақтан оңға қарай есептелінеді. Әдебиетте мұндай белгілеу кіші желі префиксі деп аталады. Мысалдар қатары 2.1-кестеде келтірілген.

Ipfwadm утилитасында ережелерді әзірлеуді қысқартатын мүмкіндігі бар. Бұл екі бағытты ережені әзірлейтін *-b* опциясы. Ол екі ережеге арналған командаларды біреуіне жинауға мүмкіндік береді:

```
# ipfwadm -F -a accept -P tcp -S 172.16.1.0/24 -D 0/0 80 -b
```

2.1-кесте

Кіші желі маскасы	Префикс
255.0.0.0	8
255.255.0.0	16
255.255.255.0	24
255.255.255.128	25
255.255.255.192	26
255.255.255.224	27
255.255.255.240	28
255.255.255.248	29
255.255.255.252	30

Енді бір ереже екі ретінде түсіндірілетін болады, тек екіншісінде желілік пакет дерекөкөзінің және қабылдаушысының мәндері орындарымен ауысатын болады.

Мұқият әзірленген ережелер жинағын қарастырайық. Онда әлі де жүйеге шабуыл жасауға болатын осал жерін анықтауға болады. Біздің ережелер жинағымыз 80 шығыс порты бар барлық пакеттерге біздің желіге кіруге мүмкіндік береді. Бұл SYN (Synchronize Sequence Numbers) орнатылған битті пакеттерге де қатысты. SYN биті TCP-пакетті қосылу сұранысы деп жариялайды. Егер сыртынан компьютерге басым қолжетімділікке ие болған болса, өзінің жағында 80 портын

қоладанатын болса, ол біздің Firewall арқылы біздің кез-келген компьютерімізге қосыла алады.

Осы мәселені шешу үшін *ipfwadm* командасында SYN биті бар пакеттерге сәйкес келетін ережелерді әзірлеуге мүмкіндік беретін параметрге ие болады. Сәйкесінше, біздің мысалда келесі қосымша ережені қосып қойған жөн:

#ipfwadm -F -a deny -P tcp -S 0/0 80 -D 172.16.10.0/24 -y #ipfwadm -F -a accept -P tcp -S 172.16.1.0/24 -D 0/0 80 -b

Y опциясы егер пакетте SYN биті орнатылған болса ғана ереженің орындалуын көрсетеді. Осылайша, жаңа ереже SYN орнатылған биті бар 80 портынан кез-келген сыртқы пакеттерді қабыл алмауды тапсырады.

Бұл арнайы ерженің негізгі ереженің алдында орналасқанына назар аударайық. IP Firewall бірінші сәйкестік қолданылатында әрекет етеді. Екі ереже де тоқтату керек пакеттерге сәйкес келеді, сол үшін бас тартатын ереженің (deny) өткізушінің алдында (accept)орналасуына көз жеткізу қажет. Кері жағдайда SYN орнатылған биті бар пакетке бас тартылмайтын болады.

Өзекті ережелерді қарау. Ережелерді енгізгеннен кейін ipfwadm оларды тізім түрінде көрсетуді сұратуға болады:

```
#    ipfwadm -F -l
```

Бұл команда тізімге барлық конфигурацияланған жіберу ережелерін енгізетін болады. Шығару шамамен мынандай болады:

```
#    ipfwadm -F -l
IP firewall    forward rules, default policy: deny
type prot      source destination                    ports
deny           tcp                                   anywhere
172.16.10.0/24                                       www ->    any
acc  tcp       172.16.1.0/24 anywhere                any ->    www
```

Шығару форматы келесідей:

- бірінші жолда ережелердің транзитті пакеттер үшін (forward rules) қолданылатындығы туралы және рұқсат ететін ережелердің әсерінен түспеген барлық пакеттер үшін үнсіз келісім бойынша тиым салатын (deny) саясаттың қолданылатындығы туралы айтылатын ортақ ақпарат болады;
- екінші жол — кестені мазмұндай (типі, протокол, дереккөз, қабылдаушы және порттар);
- келесі жолдар — ipfwadm утилитасымен берілген ережелер.

Ipfwadm командасы, егер сәйкес жазба бар болатын болса, */etc/services* қолданатын қызметтік атауға порт нөмірін таратуға талпыныс жасайтын болады.

Үнсіз келісім бойынша берілген шығыс у параметрінің әрекетін көрсетпейді. Бөлшектік шығыс үшін *-e* (extended — кеңейтілген шығыс) параметрін қолдану керек. Ол SYN пакеттеріне арналған у параметрі көрсетілетін *opt* (опциялар) бағанаға қосылады:

```
#    ipfwadm -F -l -e
P firewall forward rules, default policy: accept
pkts bytes type prot opt tosa tosx ifname ifaddress
source
0 0 deny tcp --y- 0xFF 0x00 any any anywhere 0 0 acc tcp b          0xFF 0x00 any
any 172.16.1.0/24
```

Күрделірек мысалды қарастырайық. Алдыңғы мысал өте қарапайым болды. Барлық желілік қызметтер WWW секілді қарапайым емес. Мысалға күрделірек қызметті қосайық: FTP. Ішкі желілік пайдаланушылардың Интернеттегі FTP серверлерімен жұмы істеу мүмкіндігіне ие болуы керек деген шарт қояйық: оларға

кіру, файлдарды қабылдау және тарату. Бірақ Желідегі барлық дәмелілердің барлығының біздің FTP-серверлермен жұмыс істеуіне жол беруге болмайды.

FTP сервері онда екі TCP-портының қолданылуымен қызықты: 20 (мәліметтер) және 21 (командалар):

```
# ipfwadm -a deny -P tcp -S 0/0 20 -D 172.16.1.0/24 -y
# ipfwadm -a accept -P tcp -S 172.16.1.0/24 -D 0/0 20 -b
# ipfwadm -a deny -P tcp -S 0/0 21 -D 172.16.1.0/24 -y
# ipfwadm -a accept -P tcp -S 172.16.1.0/24 -D 0/0 21 -b
```

Алайда бұл мәселені шеше қоймайды. FTP-серверлер екі әр түрлі режимде әрекет ете алады: пассивті және. *Пассивті режимде* FTP-сервер пайдаланушыдан қосылуды күтеді. *Белсенді режимде* сервер іс жүзінде пайдаланушыға қосылады. Белсенді режим әдетте үнсіз келісім бойынша берілген.

Көптеген FTP-серверлер белсенді режимде жұмыс істеген кезде 20 портынан мәліметтердің қосылуын жасайды, бұл әкімшілік ету біршама қысқартады, бірақ, өкінішке орай, барлығы мұны жасап қоймайды.

20 портына, FTP-мәліметтер портына арналған ережені толығырақ қарастырған жөн. Ережеге желінің пайдаланушысы серверге қосылған кезде жұмыс істейді. Басқаша сөзбен айтқанда, егер пассивті режим қолданылатын болса. Бұл ретте FTP-белсенді режимге жол беру үшін қанағаттанарлық ережені конфигурациялау өте қиын, себебі бұл ретте қандай порттардың қолданылатындығы анық емес.

Желі пайдаланушыларының пассивті режимді қолдануын тапсырған қауіпсіздірек болады: FTP-серверлерінің көбісі және барлық дерлік FTP-клиенттер оны қолдайды. Ішкі желіден қосылуды қабылдайтын және сыртқы қосылыстарды орнататын FTP арналған прокси-серверді қолданған – ең жақсы.

Енді *ipfwadm* бағдарламасының параметрлерін толығырақ қарастырған жөн. *Ipfwadm* командасында көптеген параметрлер бар. Синтаксистің жалпы түрі мынандай болады:

ipfwadm category(категория) command parameters [options]

Категориялар (categories). Категорияны қарастырған кезде қорғалатын желі мен сыртқы желінің (Интернеттің) арасында екі желілік интерфейсі бар компьютер орналастырылады делік, **бұл ретте олардың біреуі сыртқымен, ал басқасы – ішкі желімен өзара әрекеттесетін болады. Категориялар бапталатын ережелердің типін белгілеуге мүмкіндік береді, сәйкесінше, командадағы категория біреу ғана бола алады:**

- — I — енгізу ережесі (Input) сыртқы желіден келіп түсетін пакеттерді ғана есепке алады және оларды тағайындау мекенжайы Firewall орнатылған компьютер болып табылады;
- — ***O*** — енгізу ережесі (Output) Firewall орнатылған компьютерден шығатын және сыртқы желіге кететін пакеттерді есепке алады;
- — ***F*** — жіберу ережесі (Forwarding) сыртқы желіден ішкі желіге, және керісінше жіберілетін пакеттерді есепке алады. Командалар. Белгіленген категорияға қатысты ережелер үшін ғана қолданылады.

Команда Firewall-ға қандай әрекетті орындаған жөн екендігін көрсетеді:

- ***—a [policy]*** — ережені қосу;
- — ***i [policy]*** — ережені салу;
- — ***d [policy]*** — ережені жою;
- — ***p [policy]*** — үнсіз келісім бойынша берілген стратегияны орнату;
- — ***l*** — барлық бар ережелерді көрсету;
- — f — барлық бар ережелерді жою.

Стратегиялар (policy). Келесідей стратегиялар бар:

- ***accept*** — қабылдауға, жіберуге арналған немесе транзитті барлық пакеттерді өткізу (forward);
- ***deny*** — қабылдауға, жіберуге арналған немесе транзитті барлық пакеттерді бұғаттау(forward);
- ***reject*** — қабылдауға, жіберуге арналған немесе транзитті барлық пакеттерді бұғаттау(forward) және қателік туралы ICMP-хабарлама пакетін жіберген компьютерге жіберу.

Параметрлер. Параметрлер ереженің нақты қай пакетерге қатысты қолданылатындығын анқытайды:

- — P ***protocol*** — ***protocol*** (протокол) TCP, UDP, ICMP мәнін немесе барлық көрсетілгендерді қабылдай алады, мысалы, егер тек TCP протоколына қатысты ережені ғана қолдану талап етілетін болса, она параметр ***P tcp*** түріне ие болатын болады***;***
- ***—S address[/mask] [port]*** — пакеттің шығыс IP-мекенжайы (sourse). Егер желілік маска берілмеген болса (mask), үнсіз келісім бойынша ол ***/32*** деп қабылданады***.*** Берілген ереже қатысты болатын порттардың қосымша белгілеуге болады (port). Порттар ***/etc/services*** файлында жазылған атаулармен белгіленуі мүмкін***.*** Тізбекті нөмірлері бар бірнеше порттар келесі жолмен сипатталады:

  lowport:highport, ***мысалы: —*** S 172.29.16.1/24 ftp:ftp-data;

  - *— D address[/ mask] [port]* — тағайындалудың IP-мекенжайын көрсетеді, барлық басқа жағынан алдыңғы параметрге ұқсас болып қалады — S, мысалы: — D *172.29.16.1/24 smtp;*
  - *— V address* — пакет (— *I)* қабылданған немесе ол жіберілген (— O) желілік интерфейс мекенжайын көрсетеді, бұл шекті машинадағы кейбір таңдалған желелік интерфейстерге қатысты ғана қолданылатын ережелерді қалыптастыруға мүмкіндік береді, мысалы: — *V 172.29.16.1;*
  - *— W name* — желілік интерфейс атауын белгілейді, параметр V параметрі секілді жұмыс істейді, бірақ мекенжайдың орнына құрылғының атауы белгіленеді, мысалы: — *W ppp0*.

Параметрлердің бөлігі міндетті болып табылмайды, алайда кейде олар өте тиімді болады:

- *— b* — екі бағытталған режим үшін қолданылады, параметр белгілі бір дереккөз бен адресат арасындағы кез-келген бағытта трафикке сәйкес келеді, бұл жағдай келесі екі ережені әзірлеу қажеттілігінен айырады: біреуі тікелей қосылу үшін және біреуі кері қосылу үшін;
- *— o* — өзек протоколы арқылы пакеттердің сәйкестігін растауды қамтиды, бұл жағдайда осы ережеге сәйкес келетін кез-келген пакет өзектің рұқсат етілмеген қол жеткізуді анықтау туралы хабарламасы ретінде тіркелетін болады;
- — y — ереженің қосылу сұранысының TCP-пакеттеріне сәйкес келуі үшін қолданылады, бұл жағдайда ережеге SYN орнатылған биті бар және ACK орнатылмаған биті бар TCP-пакеттері ғана сәйкес келетін болады;
- *— k* — ереженің қосылу талпынысын растаудың TCP-пакеттеріне сәйкес келуі үшін қолданылады, сол кезде ережеге ACK орнатылған биті бар TCP-пакеттері ғана сәйкес келетін болады.

Firewall конфигурациясының әрбір командасы ICMP пакеттерінің типтерін анықтауға мүмкіндік береді. TCP және UDP порттарымен салыстырғанда

пакеттердің типтері мен олардың мәндерін жіберетін ыңғайлы конфигурация файлы жоқ. ICMP пакеттерінің типтері RFC-1700 (Assigned Numbers RFC) анықталған. Сонымен бірге олар С стандартты кітапханалық файлдарының бірінен жіберілген. GNU қарапайым кітапханасына тиесілі және ICMP протоколымен жұмыс істейтін желілік бағдарламалық қамсыздандыруды жазған кезде С-бағдарламалаушылар қолданатын */usr/include/netinet/ ip_icmp. h* файлы да ICMP пакеттерінің типтерін анықтайды. Ыңғайлылық үшін олар 2.2-кестеде келтірілген. *Iptables* командасының интерфейсі ICMP типтерін олардың аттары бойынша да анықтауға мүмкіндік береді.

2.2- кесте

Типтің нөмірі	*Iptables белгіленуі*	Сипаттамасы
0	Echo-Reply	ICMP протоколының сұраныстарын (ICMP Echo-Request) жіберген кезде көрсетілген желі түйініне жауаптар (ICMP Echo-Reply) келіп
3	Destination-Unreachable	Адресат қолжетімсіз, бұл ретте дұрыс емес немесе қол жетімсіз болуы мүмкін: желі, түйін, порт, протокол; желі объектілері әкімшілік жағынан тиым салынған және т.б.
4	Source-Quench	Дереккөзді ұстап тұру (кезекті артық толтыру кезінде дереккөзді сөндіру)
5	Redirect	Пакеттердің әр түрлі қайта бағытталуы: желіге, басқа түйінге және қызмет көрсету
8	Echo-Request	Желілік түйіннен жауапты сұрату
11	Time-Exceeded	Пакеттің тіршілік ету уақыты үзінділерді тасымалдау немесе жинау кезінде өтіп кетті
12	Parameter-Problem	Дұрыс емес параметр (пакеттің IP-тақырыпатындағы қателікпен немесе қажетті опцияның жоқ болуымен байланысты дейтаграмма параметрлері бар мәселе)
13	Timestamp-Request	Timestamp Request/ Reply хабарламалары Интернеттің әр түрлі компоненттеріндегі уақыт есептеуіштерін өзара синхрондауды қамтамасыз ету үшін арналады. Интернет компоненттерінде ортақ басқарудың болмауына байланысты компоненттің әрқайсысындағы жеке уақыт датчиктерінің мәндері айтарлықтай ерекшеленуі мүмкін. Осы датчиктерді өзара синхрондау үшін Timestamp Request/Reply хабарламалары

Типтің нөмірі	*Iptables белгіленуі*	Сипаттамасы
		Echo Request және Echo Reply хабарламаларының бірдей форматы бар және TYPE өрісінің мазмұнымен ғана ерекшеленеді. TYPE = = 14 өрісінің мәні Timestamp Reply хабарламасына сәйкес келеді, ал TYPE = 13 өрісінің мәні Timestamp Request хабарламасына сәйкес келеді
14	Timestamp-Reply	Тура сол
15	None	Ақпараттық сұраныс
16	None	Ақпараттық жауап
17	Address-Mask-Request	Мекенжайлық масканы сұрату
18	Address-Mask-Reply	Мекенжайлық масканы сұратуға жауап

2.8. IP FIREWALL CHAiNS (2.2 ядролар)

Linux операциялық жүйесі пайдаланушылардың тілектерін орындау үшін жетілдіріліп келеді. IP Firewall де бұдан өзгеше емес. IP Firewall-дың дәстүрлі нұсқасы көптеген қолданбалы бағдарламалар үшін жақсы, бірақ күрделі желілік орталарды конфигурациялау үшін тиімді бола алмайды. Осы мәселенің шешімін табу үшін «IP Firewall Chains» деп аталатын IP Firewall-ды конфигурациялаудың жаңа әдісі әзірленіп, Linux 2.2.0 ядросында жалпыға ортақ пайдалану үшін шығарылған болатын.

IP Firewall Chains пәрмені Firewall ережелер топтарын әзірлеуге жол береді, соларға жеке компьютерлер немесе желілерді қосуға және солардан алып тастауға болады. Осы тәсіл арқылы көптеген ережесі бар конфигурацияларда Firewall-дың нәтижелілігін арттырады.

IP Firewall Chains бағдарламасын 2.2 ядролар тобы ұстанады және оған ОС Linux 2.0 ядролар тобына арналған патч ретінде қол жеткізуге болады.

Ipchains пайдалану. *Ipchains* пайдаланудың екі тәсілі бар.

Бірінші тәсіл арқылы *ipchains* бағдарламасын фондық режимде басқаратын *ipfwadm*-ның орнына қолданылатын *ipfwadm-wrapper* скрипті пайдаланылады. Екінші тәсіл арқылы жаңа синтаксис қолданылып, кез келген қолнадыстағы конфигурациялар өзгертіледі.

Осындай жағдайда жаңа синтаксисті пайдалану керек. Конфигурацияны көшірген кезде оны конфигурациялауға болады. Сонымен бірге *ipchains*-тегі синтаксис *ipfwadm*-тегі синтаксистен жеңіл болады.

Ipfwadm утилитасы Firewall-ды конфигурациялау үшін тек үш ереже тобын (тізбегін) басқарып келген. IP Firewall Chains пәрмені бір-бірімен байланысқан, бірақ үш алдын-ала ереже тобы бар еркін ереже топтарын (тізбектер) жасауға болады, Бұл *ipfwadm*-да қолданылған тікелей баламалар болып табылады, тек олардың атаулары: *input, forward* және *output.*

Алдымен *ipchains* пәрменінің жалпы синтаксисін қарастыру қажет, одан кейін

тізбектің құрылу қасиеттерінің қайсыбірінде мәселе туындауын болдырмай, *ipchains* пәрменін пайдалану жолдарымен танысып шыққан жөн. Бұл әрекет келесі мысалдарға қарап орындалады.

Ipchains **пәрменінің синтаксисі.** Осы пәрменнің синтаксисі өте қарапайым:

ipchains cошmand(пәрмен) rule- зресН1са^оп(ереже сипаттамасы) options

Пәрмендер.

Пәрмендер көмегімен *ipchains*–ке арналған ережелер мен ережелер тобын басқаруға болады, көптеген жағдайда олар жоғарыда қарастырылған *fwadm* пәрменінің ережелері мен ережелер тобына ұқсас келеді. Оларды жеке қарастырып өтелік:

- —А *chain* — белгіленген тізбектің соңына бір немесе одан артық ереже қосады; егер ақпарат көзі немесе ақпарат алушы үшін машина атауы белгіленіп, ол бірнеше IP-мекен-жайына сәйкес келсе, онда ереже әрбір мекен-жайға қосылады;
- — I *chain rulenum* — бір не одан артық ереже санын белгіленген тізбектің бас жағына қосады; машина атауы ақпарат көзі немесе ақпарат алушы үшін белгіленіп, ол бірнеше IP-мекен-жайына сәйкес келсе, ондай ереже әрбір мекен-жайға қосылады;
- — D *chain* — бір не одан артық ережені белгіленген ереже сипаттамасына сәйкес келетін нақты тізбектен алып тастайды;
- — *D chain rulenum* — осы пәрмен нақты тізбектегі *rulenum* орналасқан орнындағы ережені алып тастайды, оған қоса тізбектегі бірінші ереженің алдыңғы орында (нөлдің орнында емес!) тұрғанын ескерген жөн;
- —*R chain rulenum* — осы пәрмен нақты тізбектегі *rulenum* орналасқан орнындағы ережені алмастырады;
- — С *chain* — осы пәрменбелгіленген тізбек бойынша ереже арқылы пакетті тексереді, сонымен қатар осы пәрмен тізбектің пакетті қалай өңдейтіні туралы хабарламаны өз орнына қайтарады, бұл Firewall конфигурациясын сынақтан өткізу үшін өте қолайлы, бұл кейін жеке қарастырылатын болады;
- — *L [chain]* — ешбір тізбек белгіленбесе, осы пәрмен нақты тізбектің ережесін немесе барлық тізбектер ережелерін атап шығады;
- — *F [chain]* — ешбір тізбек белгіленбесе, осы пәрмен нақты тізбектің ережесін немесе барлық тізбектер ережелерін алып тастайды;
- — *Z [chain]* — ешбір тізбек белгіленбесе, осы пәрмен нақты тізбектің ережесін немесе барлық тізбектер ережелері үшін пакеттер мен есептегішті нөлдейді;
- — *N chain* — осы пәрмен белгілі атауы бар жаңа тізбек құрайды, осылайша осы пәрмен арқылы пайдаланушы белгілеген жаңа тізбектер құрылады;
- — X *[chain]* — ешбір тізбек белгіленбесе, осы пәрмен пайдаланушының нақты тізбегін немесе барлық тізбектерді алып тастайды; сонымен бірге алынып тасталған тізбекке басқа тізбектерден сілтемелер жасалмауы тиіс,

әйтпесе ол алынып тасталмайды;

- —*P chain policy* — осы пәрмен көрсетілген тізбек үшін әдепкі қалпы бойынша нақты стратегия белгілейді, мұндағы ұйғарынды стратегиялар: ACCEPT, DENY, REJECT, REDIR немесе RETURN.

ACCEPT, DENY және REJECT стратегиялардың мәндері IP Firewall-ды әдеттегідей орындау үшін қолданылатын стратегиялардың мәндерімен бірдей. REDIR анықтағандай, пакетті Firewall пәрмені бар машинадағы порт үшін қайтадан белгілеген жөн. RETURN стратегиясы ережесі осы жағдайдың орын алуына әкелген IP Firewall-ды тізбекке қайтарып, келесі ережеден бастап оны өңдей беруді тапсырады.

Ережелерді анықтау параметрлері. *ipchains* параметрлері ереже құрастырады, сол үшін пакеттердің қай түрлерінің белгіленген өлшемдерге сәйкес келетінін анықтайды. Егер осы параметрлердің қайсыбірі ереже сипаттамасында жоқ болса, онда оның мәні әдепкі қалпы бойынша белгіленеді. Негізгі параметрлер төмендегідей:

- — *p [!]protocol* — ережеге сәйкес келетін хаттама белгілейді

(рұқсат етілген хаттама атаулары: TCP, UDP, ICMP немесе әдепкі қалпы бойынша белгіленген: ALL); осы жерде белгіленбеген хаттамалар үшін хаттама атауын белгілеуге болады (мысалы, ірір хаттамаына арналған 4 нөмірі); егер «!» префиксі белгіленген болса, онда ереже теріс болып шығады және осы хаттамаға сәйкес келмейтін барлық ережелер қабылданады;

- — *s* [!]address[/mask] [!] [port] — пакет жеткізілген бастапқы мекен-жай мен портты көрсетеді; мекен-жай машина атауын, желі атауын немесе IP-мекен-жайын белгілей алады, қалыпты пішінде (мысалы, /255.255.255.0) немесе жаңа пішінде (например, /24) белгілеуге болатын *mask* опциясы желі маскасын белгілейді, *port* опциясы TCP немесе UDP портын немесе ICMP пакеттер түрін белгілейді

  (порт сипаттамасын тек p параметрі TCP, UDP немесе ICMP хаттамалары бір-бірін белгілеген жағдайда ғана белгілеуге болады, жоғарғы және төменгі шектерді қос нүкте қойып бөлгіш ретінде белгілей отырып, порттарды ауқым деп анықтауға болады, «!» бейнесі ережені қарама-қайшы ережеге айналдырады;

- — *d* [!]address[/mask] [!] [port] — мақсатты мекен-жай мен портты белгілейді. Қалған қасиеттері бойынша s параметріне ұқсас келеді;
- —*j target* — ережесі орындалғанда пакетпен қандай әрекет орындау керектігін көрсетеді (мына іс-қимылдар жасауға рұқсат етіледі: ACCEPT, DENY, REJECT, REDIR және RETURN); пакет өңделіп жатқан пайдаланушының белгілеген тізбек атауын белгілеуге болады, егер осы параметр қалдырылған болса, онда пакеттер мен есептеуіштертегі мәліметтер ғана өзгертілетін болады, бірақ осы пакетпен ешқандай іс-әрекеттер орындалмайды;
- — *i [!]interface-name* — пакет жолдаған интерфейс немесе пакет өткізетін

интерфейсі белгілейді; «!» символы салыстырма нәтижені инверсиялайды; егер интерфейс атауы « + » нышанына аяқталса, онда атауы белгілі жолмен басталатын барлық интерфейстер оған сәйкес келеді (мысалы, — *i ppp+* PPP-интерфейстерге сәйкес келеді, ал — *i* ! *eth+* Ethernet тен басқа барлық интерфейстерге сәйкес келеді);

- [!] — f— ереженің үзіндіге бөлінген пакеттің бірінші үзіндісі үшін қолданылады.

Опциялар. *ipchains* опцияларының мәні кеңірек болады. Олар Firewall-ды конфигурациялаудың мүмкіндіктерін арттыра алатын қасиеттерге қол жеткізуге мүмкіндік береді. Солардың ең қызықтыларын қарастырып өтелік:

- — *b* — бірден екі ережені түрлендіреді, айта кететіні, біріншісі белгіленген параметрлерге дәл келеді, ал екіншісі дәл сол қызмет атқарады, бірақ қарсы бағытта қозғалатын пакеттер үшін қолданылады;
- — v —*ipchains*-ке толық ақпарат беруді тапсырады;
- — *n* —*ipchains*-ке IP-мекен-жайлары мен порттарын оларды атауларға айналдырмай-ақ пайдалануды тапсырады;
- —*1* — ережеге сәйкес келетін кез келген пакет *sysklogd* бағдарламасы арқылы өңделетін *printk()* функциясын пайдалана отырып, ядромен хаттамалайды, бұл өзгеше пакеттерді анықтау үшін өте қолайды;
- — *o[maxsize]* —*ipchains*-ті ережеге сәйкес келетін барлық пакеттерді netlink құрылғысына көшірткізеді, сонымен қатар *maxsize* параметрі netlink құрылғысына берілетін әрбір пакеттен байттар санын шегереді; осы опцияның әзірлеушілер үшін маңызы зор;
- — *m markvalue* — ережеге сәйкес келетін барлық пакеттерге таңба қойылуы тиіс (таңба арнайы белгісі жоқ 32-биттік сан болып табылады, осы опция ешқандай іс-әрекет жасап тұрған жоқ, бірақ келешекте пакеттің басқа бағдарламалық жасақтамаға қалай айналатынын анықтай алатын болады); егер таңба « + » немесе « — » тен басталса, оның мәні тиісті таңбаға қосылады немесе алып тасталады;
- — t *andmask xormask* — TOS (type of service — қызмет түрі) ережеге сәйкес келетін кез келген IP-пакетінің атауында биттерді басқаруға жол ашады; сонымен бірге қызмет түрінің биттерін интеллектуалды бағдарлауыштары пакеттерді жіберер алдында алдымен ең басымдыларын орналастыру үшін пайдаланады, ал *andmask* мен *xormask* мәндерін қызмет түрінің биттерімен бірге AND мен OR логикалық операцияларда пайдаланылатын разрядтық маскалар белгілейді;
- —x —*ipchains*-тің тұжырымындағы барлық сандар нақты болады (дөңгелектеуге болмайды);
- -y ¯ белгіленген SYN биті және белгіленбеген ACK мен FIN биттері бар кез келген TCP-пакетіне сәйкес келетін ережені белгілейді (TCP-сауалдарын іріктеу үшін пайдаланылады).

Жоғарыда қарастырылған мысалға келсек және *ipchanes* құралдары арқылы

алға қойылған тапсырманы орындасақ:

Ұйымда Интернеттен WWW серверлеріне кіруге рұқсат беретін Linux Firewall пайдаланылатын желі бар деп пайымдауға болады, бірақ бұл жерде өзге трафик блокталады.

Егер желінің 24-биттік шағын желісі (C классы) және 172.16.1.0 желі мекенжайы бар болса, онда *ipchains*-ның осындай ережелер тобын пайдалану қажет:

```
#  ipchains -F forward
#  ipchains -P forward DENY
#  ipchains -A forward -s 0/0 80 -d 172.16.1.0/24 -p tcp -y -j DENY
#  ipchains -A forward -s 172.16.1.0/24 -d 0/0 80 -p tcp -b -j ACCEPT
```

Бірінші пәрмен *forward* ережелер тобынан барлық ережелерді алып тастайды, екінші пәрмен ережелер тобына DENY дағы *forward*-қа арналған іс-қимылды әдепкі қалпы бойынша орындайды. (тек рұқсат етілген іс-қимылдар ғана орындауға болады). Үшінші және төртінші пәрмендер тиімті басқа іріктеме жүргізеді, оның үстіне төртінші пәрмен Web-серверлеріне кіруге рұқсат береді, ал үшіншісі 80 портынан TCP арқылы қосылуға бөгет жасайды.

Желі сыртындағы FTP-серверіне кірудің бейтарап режимін қамтамасыз ету қажет болған жағдайда, енгізілген параметрлерден кейін жазылатын қосымша ережелерді қосу қажет:

```
#  ipchains -A forward -s 0/0 20 -d 172.16.1.0/24 -p tcp -y -j DENY
#  ipchains -A forward -s 172.16.1.0/24 -d 0/0 20 -p tcp -b -j ACCEPT
#  ipchains -A forward -s 0/0 21 -d 172.16.1.0/24 -p tcp -y -j DENY
#  ipchains -A forward -s 172.16.1.0/24 -d 0/0 21 -p tcp -b -j ACCEPT
```

Ipchains-**те өзекті ережелерді қарап шығу**. *Ipchains* пәрменінде маңызды ережелер шығару үшін — *L argument* параметрі пайдаланылады. *Ipfwadm* пәрмені сияқты мұнда тұжырымдаманы талдауға мүмкіндік беретін дәлелдер келтірілуі мүмкін. Ең қарапайым жағдайда *ipchains* пәрмені мына нәтиже шығарады:

```
#  ipchains -L -n
Chain input (policy ACCEPT):
Chain forward (policy DENY):
target prot opt source destination ports
DENY tcp -y----------  0.0.0.0/0              172.16.1.0/24 80 -> *
ACCEPT tcp  ---------- 172.16.1.0/24 0.0.0.0/0                    * -> 80
ACCEPT tcp  ---------- 0.0.0.0/0              172.16.1.0/24       80 ->*
ACCEPT tcp  ---------- 172.16.1.0/24 0.0.0.0/0                    * -> 20
ACCEPT tcp  ---------- 0.0.0.0/0              172.16.1.0/24       20 ->*
ACCEPT tcp  ---------- 172.16.1.0/24 0.0.0.0/0                    * -> 21
ACCEPT tcp  ---------- 0.0.0.0/0              172.16.1.0/24       21 ->*
Chain output (policy ACCEPT):
```

Ешбір тізбектің атауы белгіленбесе, онда *ipchains* пәрмені тізбектерден барлық ережені шығарады (біздің жағдайда бұл *input, forward* және *output* тізбектері, яғни, тек *forward* тізбегі үшін ғана ережелер енгізілген). Мысалымызда *n* параметрі оның тиісті мекен-жай немесе портты тиісті атауға айналдырмағаны туралы *ipchains* пәрменіне хабар береді.

u опциясы арқылы шақырылған толық нысан көбірек бөлшек шығаруға мүмкіндік береді. Шығарылған тұжырымдама пакеттер мен байттар есептегішеріне, Type of Service AND және XOR маскаларына, интерфейс атауы мен таңбалар мәндеріне арналған өрістер қосады.

Ipchains пәрмені арқылы құрастырылған барлық ережелердің өзінің пакеттері мен пакеттермен байланысқан байт есептегіштері бар. Бұл желілік трафик есебін жүргізуге жол ашатын IP Accounting үшін маңызды. Әдепкі қалпы бойынша осы есептегіштер мәліметтерді мыңдап және миллиондап көрсетуі үшін K және M суффикстерін пайдаланатын дөңгелек пішіндес болып келеді. Егер x аргументі белгіленген болса, онда есептегіштер дөңгелектемей-ақ жұмыс істей береді.

ipchains пәрмені пәрменлық тармағы бар қарапайымдырақ синтаксисі мен кейбір қызықты кеңейтілімдері бар *ipfwadm* пәрменін алмастырады, бірақ пайдаланушы анықтаған тізбектер не үшін қажет болғаны белгісіз. *Ipchains*-тарға қолдау көрсететін скрипттерді пайдалану жолдарын қарастырған жөн.

Пайдаланушы анықтайтын тізбектер.

Кәдімгі IP Firewall тізбегі үш ереже тобын оңай түсінуге болатын және қарапайым Firewall талаптары қойылған кішігірім желілер үшін қолайлы болып табылатын Firewall конфигурациясының қалыптасу механизмін қамтамасыз етеді.

Алайда ірі желілерде маңызды мәселелер мен талаптар туындайтыны сөзсіз. Ережелер топтары "жентек қар" тәрізді өсе береді және оларды басқару қиынға соғады. Ең нашары – ережелер сандары өскен сайын, IP Firewall-дың нәтижелілігі төмендей түседі, себебі бағдарламаға әрбір пакетті ережелердің үлкен сандарымен салыстыруға тура келеді. Оның үстіне, ережелер тобын қауіпсіз түрде өшіруге болмайды. Оның орнына, кей топтаманы өшіруіңізге тура келеді, оны ауыстырып отырған кезде, желіге әркім кіре алады!

Жаңа IP Firewall тізбектерін жасау арқылы осы мәселелердің барлығын шешуге болады. Әрбір осындай тізбек енгізілген тізбектермен бірге қолданыла алады. Сегізден аспайтын символдан құралған атауы бар жаңа тізбек құру үшін *ipchains* пәрменінің параметрлерін пайдалануға болады. Тек жаңа тіркелімнің символдарынан ғана туратын атау да жаман емес болар. *j* опциясы пакеттің осы ережеге жауабын белгілеуге жол ашады. Пакет осы ережеге сәйкес келсе, ол пайдаланушы белгілеген ереже бойынша сынақтан өту керек деп деп пайымдайды.

Жаңа ережелер тізбегін жасай алатын *ipchains* пәрмендерінің ретін қарастырып өтелік:

ssh -j ACCEPT www - j ACCEPT

```
# ipchains -P input DENY
# ipchains -N tcpin
# ipchains -A tcpin -s ! 172. L6.0.0/16
# ipchains -A tcpin -p tcp -d 172.16.0. 0/16
# ipchains -A tcpin -p tcp -d 172.16.0. 0/16
# ipchains -A input -p ftoor tcpin
# ipchains -A input -p all
```

Бірінші пәрменде әдепкі қалпы бойынша *input* ережелер тобы үшін қолданылатын DENY стратегиясы белгіленген.

Екінші пәрмен пайдаланушы анықтаған және жергілікті тораптың сыртынан келген кез келген пакетке сәйкес келетін жаңа *tcpin* тізбегін құрайды.

Үшінші пәрмен оған әлі де ешқандай іс-қимыл орындамайтын ереже қосады. Бұл ереже тек есеп жасау үшін ғана қажет.

Төртінші және бесінші пәрмендер жергілікті торап үшін және ssh немесе www порттарының кез келгені үшін арналған кез келген пакетке сәйкес келеді, осындай пакеттер қабылданады.

Алтыншы ереже *ipchains* пәрменінің жаңа мүмкіндіктерін көрсетеді. Ол TCP хаттамасының барлық кіріс пакеттері үшін іске қосылады және оларды пайдаланушы анықтаған *tcpin* тізбегіне жолдайды.

input тобына қосылған жетінші ереже кез келген пакетке сәйкес келеді, ешқандай іс-қимыл жасамайды және есеп жасау үшін арналған.

input және *tcpin* ережелер тобы енгізілген ережелерді қамтиды. Пакетті өңдеу үрдісі әрқашан енгізілген тізбектерден басталады. Пайдаланушының тізбегі енгізілген тізбектердің бірінің пәрмені бойынша тораптық пакеттерді өңдеу үрдісіне енеді. UDP пакет алынған кезде не болатынын қарастырып өтелік. Әуелі пакет *input* тізбегіне өтеді. *Input* тізбегінің алғашқы ережесі (ережелер жазбасындағы алтыншысы) оны ескермейді, себебі ол тек қана TCP пакеттерін өңдеп шығады. Пакет екінші *input*-тегі ережеге сәйкес келеді, бірақ ол жолданушыны анықтамайды, себебі байттар мен пакеттер есептегіштерін құр түрлендіреді және пакетпен ешқандай іс-әрекеттер жасамайды. Ол *input* соңына дейін жетіп, әдепкі қалпы бойынша белгіленген *input* (DENY) арналған стратегиямен кездесіп, ауытқып кетеді.

Енді *ssh* портына арналған TCP-пакет келгенде не болатынын қарастырып өтелік. Осы жолы *input* тізбегіндегі екінші ереже сәйкес келеді және пакетті *tcpin* (пайдаланушы анықтаған тізбекке) тізбегіне жолдау жолын анықтайды.

Пайдаланушы анықтаған тізбекті жолданушы етіп белгілеу арқылы пакет сол тізбектегі ережелер бойынша тексеріледі, сондықтан келесі тексерілетін ереже - *tcpin* пәрменіндегі бірінші ереже болып табылады. Бірінші ереже бастапқы мекен-жайы жергілікті желінің сыртында орналасқан және ешқандай жолданушы анықталмаған пакетке сәйкес келеді, сондықтан бұл да есеп ережесі болып табылады және келесі ереже сынақтан өтеді. *tcpin* пайдаланушының тізбегіндегі екінші ереже осы пакетке сәйкес келеді және ACCEPT іс-қимылын анықтайды. Осылайша, пакет қабылданған болып саналады.

Қорытындылай келе, пайдаланушы белгілейтін тізбектің соңына дейін жеткенде не болатынын қарастырған жөн. Сол үшін белгіленген ережелерге сәйкес келмейтін кіріс пакетінің тәртібін зерттеп өтелік. Бұл **telnet**-ке арналған сауал болсын.

Пайдаланушы анықтаған тізбектерде әдепкі қалпы бойынша анықталған сыртқы қоздырғыштарға сезгіштігі жоқ. Пайдаланушы анықтаған тізбектегі барлық ережелер тексерістен өткен кезде, және ешқайсысы да орын алған жағдайға сәйкес келмесе, RETURN ережесімен белгіленген тәрізді Firewall іске қосылады. Біздің мысалда тексеріс *input* тобына қайта оралады. Ақыр соңында, әдепкі қалпы бойынша белгіленген DENY стратегиясы бар пакет *input* тізбек соңына дейін жетеді де, ауытқиды.

Бұл мысал өте қарапайым, бірақ жұмыстың негізгі қағидасын көрсетеді. Бұдан күрделі мысалды қарастырып өтелік:

```
#  Транзитті пакеттер үшін мына тәртіпті орнатайық:
REJECT ipchains -P forward REJECT
#
#  Төрт пайдаланушылық тізбек құрайық:
        ipchains -N sshin ipchains -
        N sshout ipchains -N
        wwwin ipchains -N
        wwwout
#
#  Орнатылған SYN биті бар пакеттерге қызмет көрсетуден бас тартуды
қамтамасыз етейік:
        ipchains -A wwwin -p tcp -s 172.16.0.0/16 -y - j REJECT
        ipchains -A wwwout -p tcp -d 172.16.0.0/16 -y - j REJECT
        ipchains -A sshin -p tcp -s 172.16.0.0/16 -y - j REJECT
        ipchains -A sshout -p tcp -d 172.16.0.0/16 -y - j REJECT
#  Тізбектердің соңына дейін жеткен пакеттердің шығарылуын қамтамасыз етеміз:
        ipchains -A sshin -j REJECT ipchains -A
        sshout -j REJECT ipchains -A wwwin -j
        REJECT ipchains -A wwwout -j REJECT
#  www және ssh пакеттерін тиісті тізбекке жолдаймыз:
        ipchains -A forward -p tcp -d 172.16.0.0/16 ssh -b -j sshin
        ipchains -A forward -p tcp -s 172.16.0.0/16 -d 0/0 ssh -b -j sshout
        ipchains -A forward -p tcp -d 172.16.0.0/16 www -b -j wwwin
        ipchains -A forward -p tcp -s 172.16.0.0/16 -d 0/0 www -b - j wwwout
#  Нақты машиналарға арналған ережелерді тізбектегі екінші орынға қоямыз
        ipchains -I wwwin 2 -d 172.16.1.2 -b -j ACCEPT ipchains -I wwwout 2 -s
        172.16.1.0/24 -b -j ACCEPT ipchains -I sshin 2 -d 172.16.1.4 -b -j ACCEPT
        ipchains -I sshout 2 -s 172.16.1.4 -b -j ACCEPT ip-chains -I sshout 2 -s
        172.16.1.6 -b -j ACCEPT
```

Мысалда Firewall конфигурациясын басқаруды жеңілдету және енгізілген тізбектерді ғана қамтитын шешімге қарағанда оның тиімділігін арттыру үшін пайдаланушы анықтаған тізбектер таңдалған.

Мысалда қосылудың әрбір бағытындағы *ssh* және *www* сервистеріне арналған пайдаланушы анықтаған тізбектер құрылған. *wwwout* тізбегіне World Wide Web сервер арқылы қосылуға рұқсаты бар компьютерлерге арналған ережелер мен *ssh* кіріп қосыла алатын машиналарға арналған ережелерді орындайтын *sshin* тізбегі орналастырылған. Тораптағы әрбір компьютер үшін осы қосылуларды икемділікпен белгілеу қажет. Бұл кейін жеңіл болады, себебі пайдаланушы анықтаған тізбектері кіріс және шығыс пакеттерінің компьютерлерден кіру құқықтары бойынша ережелерді мұқият топтастыруға жол береді.

Мұның нәтижелілігі арта түседі, себебі жолданушыны табу үшін қажетті кез келген пакет үшін сынақтардың орта саны азая түседі. Пайдаланушы анықтаған тізбегінсіз әрбір пакетпен қандай іс-әрекет жасау керектігін анықтау үшін ережелердің толық тізімін қарап шығуға тура келеді. Егер тексерілетін пакет енгізілген тізбектегі қарапайым ережеге сәйкес келмесе, пайдаланушының анықтаған тізбектері көптеген ережелердің тексерілуін болдырмайды.

***Ipchains* қолдау скриптері**. *Ipchains* пакетінің үш қолдау скриптісі бар. Солардың бірі жоғарыда қысқаша қарастырылған, ал қалған екеуі Firewall конфигурациясын сақтау және қалпына келтірудің қарапайым әрі қолайлы жолдарын қамтамасыз етеді.

ipfwadm-wrapper скриптісі *ipfwadm* пәрменінің пәрмендік тармағының синтаксисін эмульдайды, бірақ шын мәнісінде Firewall ережелерін құрастыру үшін *ipchains* пәрменін іске қосады. Бұл қолданыстағы Firewall конфигурациясын жаңа ядроға ауыстырудың және *ipchains* синтаксисін зерттеудің қолайлы әдісі. *ipfwadm-wrapper* скриптінің мінез құлқы екі бөлшекте де *ipfwadm* пәрменінен өзгеше болады. Біріншіден, *ipchains* пәрмені мекен-жай бойынша интерфейс сипаттамасын ұстанбайтындықтан, *ipfwadm- wrapper* - V параметрін қабылдайды да, бірақ оны белгіленген мекен-жайы бар интерфейс атауын іздей отырып, *ipchains* баламасына *-W* түрлендіруге тырысады. V опциясы пайдаланған кезде *ipfwadm-wrapper* скриптісі ескерту шығарып тұрады. Екіншіден, есеп жасау ережелерінің үзінділері дұрыс таратылмайды.

ipchains-save және *ipchains-restore* скриптілері Firewall конфигурациясының құрылуы мен өзгеруін одан жеңіл етеді. *ipchains- save* пәрмені қолданыстағы Firewall конфигурациясын оқиды және жеңілдетілген нысанды стандартты тұжырымдамаға жазады. *ipchains-restore* пәрмені *ipchains-save* пәрменінің шығыс форматындағы мәліметтерін оқып, IP Firewall конфигурациясын осы ережелерге сәйкес белгілейді. Осы скриптерді пайдаланудың артықшылығы – конфигурацияны серпінді өзгертуге, одан кейін оны файлда сақтау мүмкіндігінде.

Конфигурацияны сақтау үшін, мынаны енгізу қажет:

ipchains-save >/var/state/ipchains/firewall.state

Жүктеу барысында оларды мына пәрмен арқылы қалпына келтіруге болады:

ipchains-restore </var/state/ipchains/firewall.state

ipchains-restore скриптісі пайдаланушы анықтаған барлық тізбектердің бар екендігін тексереді. Егер белгіленген параметр — f болып жатса, онда ол баптаудан бұрын пайдаланушының тобынан барлық ережелерді автоматты түрде өшіріп тастайды. Әдепкі қалпы бойынша тізбекті тазартуды растау үшін сауал жолданады.

2.9. NETFILTER ЖӘНЕ IP КЕСТЕЛЕР (2.4 ядролар)

IP Firewall Chains ті әзірлеген кезде Пауль Рассел (Paul Russell) что IP Firewall қарапайым болу керек деп шешті. Ол фильтр кодын жетілдіре бастады және одан әлдеқайда қарапайым және мықты пакет жасады — netfilter.

IP Chains-терде туындайтын мәселелер. IP Chains-тер Firewall ережелерін басқарудың нәтижелілігін айтарлықтай арттырған болатын. Алайда олар пакеттерді, әсіресе, Firewall-дың басқа мүмкіндіктерімен бірге, мысалы, IP Masquerade және мекен-жай көрсетілімінің басқа нысандарымен бірге өте ұзақ өңдеп отырған. Осы мәселенің орын алуының себебі - IP Masquerade (IP маскалау) және Network Address Translation (мекен-жайларды желі бойынша аудару) IP Firewall-ге қарастан әзірленіп, оған енгізілген болатын.

Оған қоса, басқа да мәселелер пайда болды. Атап айтқанда, *input* ережелер тобы IP деңгейінің кіріс ағымын біртұтас етіп сипаттаған. Бұл топтама осы компьютерге арналған пакеттерге де, оған кейін берілетін пакеттерге де әсерін тигізген. Бұл дұрыс емес, себебі осы әдіс *input* тізбегінің функциясын шығыс пакеттер үшін қолданылатын *forward* тізбегінің функциясымен біріктірген. Кіріс пакеттер мен көрсетілген пакеттерді түрлі амалмен өңдеудің ең күрделі конфигурациялары пайда болған.

Басқа мәселе – іріктеу тетігі жүйе ядросында орналасқан және оның жұмыс логикасын ядроны толығымен қайта өңдемей-ақ өзгерту мүмкін емес еді. Осылайша, ядроға іріктеу логикасы ерекше қосымша модульдер енгізуге жол беретін netfilter пайда болған және оның баптау сызбасы қарапайым.

Басты ерекшелігі – ядродан IP маскалауға арналған кодты шығару және *input* мен *output* ережелері тобы жұмысындағы логиканың өзгеруінде. *iptables* конфигурациялаудың кеңейтілген аспабы пайда болған.

IP Chains-нд *input* ережелер тобы компьютер үшін алынғанына немесе басқа компьютерге жіберілгеніне қарамастан жергілікті компьютер арқылы алынған барлық пакетте үшін қолданылады. Netfilter-дегі *input* ережелер тобы жергілікті компьютерге арналған пакеттер үшін ғана қолданылады. *Forward* тізбегі енді басқа компьютерге таратуға арналған пакеттер үшін қолданылады. IP ^ains де ережелер тобы *output* жергілікті компьютерде түрленгеніне/түрленбегеніне қарамастан компьютерден келіп түскен барлық пакеттер үшін қолданылады. Netfilter-де осы топтама тек қана осы компьютерде түрленген пакеттер үшін қолданылады да, транзитпен өтетін пакеттер үшін қолданылмайды. Бұл өзгеріс баптау процессін күрт өзгерткен болатын.

IP маскаланған жұмыс компоненттерін ядроның бөлек модульдеріне шығару – жаңалыққа айналды. Олар netfilter модульдері болып көшірілген.

әдепкі қалпы бойынша ***input***, ***forward*** және ***output*** үшін ***deny*** стратегиясы белгіленген конфигурация жағдайын қарастырып өтелік. ***Ipchains*** те барлық пакеттерді өткізу үшін алты ережені орындауы қажет еді.

netfilter де бұл мәселелер азаяды. Firewall арқылы өтуі тиіс, бірақ компьютерде аяқталмайтын пакеттер үшін ***forward*** тобындағы тек екі ереже қажет болып тұр*:* біреуі тікелей, ал біреуі кері өткізу үшін.

ipfwadm **және** *ipchains* **мен кері сыйысушылық**. Linux netfilter дің асқан икемділігі ***ipfwadm*** және ***ipchains***, интерфейстерін эмульдау қасиетімен көрсетіледі, бұл Firewall бағдарламалық жабдықтаманың келесі ұрпағына өтуін жеңілдетеді.

ipfwadm. o және ***ipchains. o*** атаулы netfilter-ден алынған екі модуль ядросы ***ipfwadm*** және ***ipchains*** мен кері сыйысушылықты қамтамасыз етеді. Осы модульдердің тек біреуін ғана бір мезетте жүктеп алуға және оны ***ip_tables. o*** модулі жүктелмесе ғана пайдалануға болады. Тиісті модуль жүктелген жағдайда, netfilter-дің жұмысы белгіленген Firewall-дің жұмысына ұқсас болады.

netfilter ***ipchains*** интерфейсін эмульдауы үшін мына пәрмендерді енгізу қажет:

```
# rmmod ip tables
# modprobe ipchains
# ipchains
```

iptables-**тың қолданылуы**. ***iptables*** утилитасы netfilter ережелерін баптау үшін қолданылады. Синтаксис ***ipchains***-тен алынған, бірақ оның бір маңызды ерекшелігі бар: ол кеңейтілуі мүмкін, яғни оның функционалдық мүмкіндіктері пакетті қайта құрастырмай-ақ кеңейтілуі мүмкін. Сол үшін арнайы кітапханалар қолданылады және стандартты кеңейтілімдері бар.

iptables пәрменін қолданар алдында netfilter ядросының модулін жүктеп алған жөн, бұл пәрменге жұмыс істеуге көмектеседі. Осы әрекетті ***modprobe***

пәрмені арқылы орындаған оңай:

```
# modprobe ip tables
```

iptables пәрмені IP Filter мен Network Address Translation баптау үшін қолданылады. Сол үшін екі кесте қолданылады: filter және nat. егер — t опциясы белгіленсе, filter кестесі қолданылады. Бес енгізілген тізбек бар (ережелер тобы): INPUT және FORWARD — filter кестесіне арналған, PREROUTING және POSTROUTING — nat кестесіне арналған және OUTPUT — барлық кестелерге арналған.

Iptables пәрмендерінің синтаксисі жалпы осындай болады:

```
iptables command rule-specification extensions
```

Кейбір параметрлерді толық қарастырып өтелік, одан кейін мысалдарды қарастыра бастаймыз.

Пәрмендер. Пәрмендер *iptables* ережелер мен ережелер тобын басқаруға мүмкіндік береді. IP Firewall-ға мыналар жатады:

- —*A chain* — пәрмені белгіленген тізбектің соңына бір не одан артық ереже қосады; егер машина атауы мәлімет көзі немесе жолданушы үшін белгіленген болса, және бірнеше IP-мекен-жайына сәйкес келетін болса, онда ереже әрбір мекен-жай үшін қосылатын болады;
- —*I chain rulenum* — пәрмені белгіленген тізбектің басына бір не одан артық ереже қосады; егер мәлімет көзі немесе жолданушы үшін машина атауы белгіленген болса, және бірнеше IP-мекен-жайына сәйкес келетін болса, онда ереже әрбір мекен-жайға қосылатын болады;
- — D *chain* — пәрмені белгіленген ереже сипаттамасына сәйкес келетін бір не одан артық ережені белгілі бір тізбектен алып тастайды;
- — *D chain rulenum* — пәрмені көрсетілген тізбектің *rulenum* орналасқан орнындағы ережені алып тастайды, бұл жерде нөмірлер 1-ден басталады;
- —*R chain rulenum* — пәрмені көрсетілген тізбектің *rulenum* орналасқан орнындағы ережені белгіленген ережемен алмастырады;
- — *C chain* — пәрмені белгіленген тізбек бойынша ереже сипаттамасының көмегімен пакетті тексереді; бұл пәрмен пакеттің тізбек арқылы өңделуі туралы хабарламаны орнына қайтарады, бұл Firewall конфигурациясын тестілеу үшін пайдаланылады;
- — *L [chain]* — егер нақты ережелер тобы белгіленбеген болса, топтамадағы ережелер немесе барлық ережелерді шығарады;
- — *F [chain]* — егер нақты ереже тобы белгіленбесе, топтамадағы немесе барлық топтардағы ережені өшіріп тастайды;
- — *Z [chain]* — егер нақты ереже тобы белгіленбесе, топтағы барлық ережелер үшін пакеттер мен байттар есептегішін нөлге келтіреді;
- — *N chain* — белгіленген атауы бар жаңа тізбек құрайды;
- —*X [chain]* — нақты тізбек белгіленбесе, нақты пайдаланушының тізбегін немесе барлық тізбектерді өшіріп тастайды; бұл жерде өшірілетін тізбекке басқа тізбектерден сілтемелер жасалмауы тиіс, әйтпесе ол өшірілетін болады;

- — *P chain policy* —әдепкі қалпы бойынша көрсетілген тізбек үшін стратегия белгілейді (рұқсат етілген стратегиялар: ACCEPT, DROP, QUEUE және RETURN; ACCEPT пакет өткізеді; DROP пакетті лақтырып тастайды; QUEUE пайдаланушының тізбегіне пакетті өңдеуге тапсырады; RETURN пәрмені ережесі осы жағдайды туғызған IP Firewall-ды тізбекке оралуды және оны келесі ережеден бастап өңдей беруді тапсырады).

Ережелерді анықтау параметрлері. ***iptables*** параметрі пакеттердің қандай түрлері өлшемдерге сай келетінін анықтау арқылы ережелер құрастырады. Егер осы параметрлердің қайсыбірі ереже сипаттамасынан түсірілсе, онда ол әдепкі қалпы бойынша белгіленеді. Ережелер анықтаудың келесі параметрлері ажыратылған:

- — ***p*** *[\]****protocol*** — ережеге сәйкес келетін хаттаманы көрсетеді (TCP, UDP, ICMP хаттамаларының рұқсат етілген мәндері, барлық хаттамалар мәндер әдепкі қалпы бойынша белгіленеді); бұл жерде осы белгіленбеген хаттамалар үшін хаттама нөмірін белгілеуге болады (мысалы, IPIP хаттама үшін 4); егер «!» префиксі белгіленбесе, онда ереже теріс ережеге айналады және осы хаттамаға сәйкес келмейтін барлық пакеттер қабылданады;
- — ***s*** [!]address[/mask] — пакет келіп түскен бастапқы мекен-жай мен портты көрсетеді (мекен-жай машина атауын, желі атауы немесе IP-мекен-жайын белгілей алады); ***mask*** опциясы желілік масканы белгілейді (қалыпты нысанда белгіленуі мүмкін, мысалы, /255.255.255.0, немесе жаңа нысанда белгіленуі мүмкін, мысалы, /24), ***port*** опциясы TCP порты немесе UDP порты немесе ICMP пакеттер типін (егер TCP, UDP немесе ICMP хаттамаларымен бірге — ***p*** параметр белгіленбесе, порт сипаттамасын белгілеуге болады) белгілейді; порттар ауқым болып белгіленуі мүмкін, бұл жерде ауқымның жоғарғы және төменгі шектерін бөлгіш ретінде қос нүктемен бірге белгілейді (мысалы, 20:25 порттарды 20 дан 25 дейін (қоса алғанда) белгілейді), «!» нышаны ережені кереғарына айналдырады;
- — ***d*** [!]address[/mask] — мақсатты мекен-жай мен портты белгілейді, басқа жағдайларда — s параметріне ұқсас келеді;
- —j ***target*** — ереже іске қосылған кезде қандай әрекеттер жасау керектігін көрсетеді(рұқсат етілген әрекеттер: ACCEPT, DROP, QUEUE және RETURN жоғарыда сипатталған); бұл жерде пайдаланушы анықтаған атауды белгілеуге болады, сол атауда өңдеу жүре береді, ал егер бұл параметр түсіп қалған болса, онда пакеттер мен есептегіштердің мәліметтері өзгертіліп, осы пакетпен ешқандай іс-әрекет жасалмайды;
- — ***i*** [!]***interface-name*** — пакет келіп түскен немесе пакетті өткізетін интерфейсті белгілейді; «!» нышаны салыстырманың нәтижелерін инверсиялайды, бұл жерде интерфейс атауы « + » ға аяқталса, оған атаулары « + » нышанының алдында тұрған жолдан басталатын барлық интерфейстер сәйкес келеді (мысалы, — ***i ppp***+ барлық PPP-интерфейстерге сәйкес келеді, ал — ***i*** ! ***eth***+ Ethernet-тен басқа барлық интерфейстерге сәйкес келеді);

- — ***o*** [!]***interface-name*** — пакеттер атауды көрсете отырып, интерфейс арқылы таратыратынын көрсетеді, басқа жағдайларда — і ға ұқсас келеді;
- [!] — f — осы ередженің пакеттің бірінші үзінділеріне емес, екінші және одан кейінгіге үшін қолданылатынын көрсетеді.

Опциялар. *iptables* опцияларының мағынасы кеңірек болады. Олар осы бағдарламаны конфигурациялар мүмкіндіктерін айтарлықтай кеңейтеді:

- — v —*iptables* пәрменіне толық ақпарат беруді тапсырады;
- — *n* —*iptables* пәрменіне IP-мекен-жайы мен порттарды пайдалануды тапсырады да, оларды жеке атауларға түрлендірмей-ақ қояды;
- — *x* —*iptables* пәрмені шыққан кезде барлық сандар нақты болады (дөңгелектенбейді);
- — *-line-numbers* — ережелер тобын бейнелеп көрсету қажет болған кезде жолдар нөмірлерін белгілейді, бұл жерде жол нөмірі тізбек ішіндегі ереженің орналасқан қалпына сәйкес келеді.
- **Кеңейтілімдер (extensions).** Жоғарыда аталғандай, *iptables* модульдер арқылы кеңейтіледі. *ipchains* қосымша қасиеттерінің кейбіреулерін қамтамасыз ететін кеңейтілімдер стандарты бар. Кеңейтілімді пайдалану мүмкіндігін алу үшін *iptables*-та — *m name* параметр арқылы атауды анықтау қажет. Келесі кесте контексттің кеңейтілімін орнататын — *m* мен — р опцияларды көрсетеді:

1) TCP-кеңейтілім — *m tcp* мен — *p* опцияларымен бірге пайдаланылады.
   tcp:
   - — —*sport* [!] [port[:port]] — осы ережеге сәйкес келу үшін пакеттер көзін пайдалануы тиіс портты анықтайды; жоғарғы және төменгі шектерді көрсете отырып ауқымды белгілеу рұқсат етіледі (мысалы: 20:25 20-тен 25-ке дейінгі (қоса алғанда) барлық порттарды белгілейді), «!» нышаны мәнді инверсиялайды;
   - — —*dport* [!] [port[:port]] — шығыс пакеттер пайдалануы тиіс портты белгілейді. Басқа жағдайларда — — *sport* -а ұқсас келеді.
   - — —*tcp-flags* [!] *mask comp* — TCP-пакетіндегі жалаушалар *mask* мен *comp*; анықтамаларға сәйкес келгенде осы ереже қолданылатынын анықтайды, мұндағы *mask* (үтір арқылы) жалаушалар тізімін белгілейді, ал *comp* солардың жағдайын көрсетеді (рұқсат етілген жалаушалар: SYN, ACK, FIN, RST, URG, PSH, ALL немесе NONE), «!» нышаны әдетте барлық ережелер үшін қолданылады — ол мәнді инверсиялайды;
   - [!] — — *syn* — пакеттегі 1 жалаушаға SYN және 0 жалаушаға ACK мен FIN қойылуы тиіс деп анықтайды, осылайша, көрсетілген параметрлердің осындай мәндері бар пакет TCP-қосылу үшін пайдаланылады және осы опцияны қосылу үшін келіп түскен сауалдарды сәйкестендіру үшін қолдануға болады;

2) UDP-кеңейтілімдері —— *m udp* мен —*p udp:* опцияларымен бірге қолдану
   - — —*sport* [!] *[port[:port]]* — осы ережеге сәйкес келу үшін пакеттер

көзі пайдаланатын портты анықтайды; бұл жерде жоғарғы және төменгі шектерді көрсете отырып, ауқым белгілеуге болады (мысалы, 20:25 20 тен 25 дейінгі (қоса алғанда) барлық порттарды белгілейді), «!» нышаны мәнді инверсиялайды;

- — —*dport* [!] [port[:port]] — шығыс пакеттері пайдаланатын портты белгілейді, басқа жағдайларда — —*sport* -на ұқсас келеді.

3) ICMP-кеңейтілімі —— *m icmp —p icmp:* опцияларымен бірге қолданылады.

- — — icmp-type [!] *typename* — осы ережеге сәйкес келетін ICMP-хабарламаларын көрсетеді, бұл жерде хабарламалар түрлерін нөмірлер немесе атаулармен белгілеуге болады (рұқсат етілген атаулар: *echo-request, echo-reply, source-quench, time- exceeded, destination-unreachable, network-unreachable, host- unreachable, protocol-unreachable* и *port-unreachable);*

4) MAC-кеңейтілімі — — *m* mac опцияларымен пайдаланылады:

- — — *mac-source* [!] *address* — Ethernet желісіндегі қандай мекен-жайдан осы ереже үшін пакет келуі тиіс екендігін анықтайды, тек *input* немесе *forward* ережелері үшін ғана мәні зор, себебі кез келген таратылған пакет *output* ережелеріне сәйкес келуі тиіс.

Қолданылған мысалдар.

Есіңізге сала кетейік, netfilter сүзгішін пайдаланған кезде *ipchains. o* модулін оңай жүктеуге болады да, онымен *ipchains.* мен сияқты жұмыс істеуге болады. Осының орнына *iptables* пайдаланып, жоғарыда анықталған ережелерді қайтадан жазып шығамыз.

Кей ұйымның желісі бар деп жорамалдаймыз, Linux-машинада Firewall іске қосылған. Барлық ішкі пайдаланушылар Интернеттегі тек WWW-серверлеріне кіре алады.

Егер желі 24 битті (С санаптағы) желілік маска пайдаланатын және желісінің мекен-жайы 172.16.1.0 болса, онда келесі *iptables* ережелерін пайдалану керек:

```
#  modprobe ip tables
#  iptables -F FORWARD
#  iptables -P FORWARD DROP
#  iptables -A FORWARD -m tcp -p tcp -s 0/0 --sport 80 \
-d 172.16.1.0/24 / --syn -j DROP
#   iptables -A FORWARD -m tcp -p tcp -s 172.16.1.0/24 --sport / 80 \
-d 0/0 -j ACCEPT
#   iptables -A FORWARD -m tcp -p tcp -d 172.16.1.0/24 --dport 80 \
-s 0/0 -j / ACCEPT
```

Келтірілген мысалда *iptables* пәрмені дәл *ipchains* пәрмені сияқты жұмыс істейді. Жалғыз ерекшелігі - *ip_tables. o* модулін алдын ала жүктеу қажеттілігінде.

Назар аударыңыз, *iptables* модулі — b опциясын ұстанбайды, сондықтан әрбір бағыт үшін бөлек ереже белгілеу керек.

TOS биттерін басқару. Қызмет көрсету түрлерінің биттері (Type Of Service — TOS) IP-пакетінің атауындағы 4 битті жалаушадан құралған топтама болып табылады. Осы жалаушалалардың қайбірі орнатылғанда, бағдарлауыштар осы пакетті TOS-биттер тобы жоқ пакетке қарағанда басқаша өңдей алады. Төрт биттің әрқайсысының мақсаты әр түрлі, тек TOS-биттердің біреуі ғана нақты уақытта орнатылуы мүмкін. Жалаушалар қызмет көрсету түрлері деп аталады, себебі олар мәлімет таратын қолданбалы бағдарламаға талап етілген желілік қызмет көрсету түрін желіге хабарлауға мүмкіндік береді.

Желіге қызмет көрсетудің келесі түрлері бар:

- *Minimum Delay* — пәрмені бастапқы компьютерден жолданушының мекенжайына пакет жеткізу уақыты (күту уақыты) ең маңызды болғанда пайдаланылады, бұл жерде жеткізуші осындай пакеттерді жеткізу үшін ең шапшаң байланыс арнасын таңдайды;
- *Maximum Throughput* — пәрмені қолданбалы тапсырманың жұмысы сәтті орындалуы үшін мәлімет тарату арнасының өткізгіштік қасиеті маңызды болғанда пайдаланылады;
- *Maximum Reliability* — пәрмені мәліметтер жолданушыға қайта-қайта жібермей-ақ бірден жететінін анықтау үшін пайдаланылады;
- *Minimum Cost* — пәрмені мәлімет тарату құнын азайту керек болғанда пайдаланылады, бұл жерде жеткізушінің неше түрлі арналары болуы мүмкін және жеткізуші арзан арнасы арқылы трафик жолдай алады. **TOS-биттерін** *ipfwadm* **немесе** *ipchains.* көмегімен белгілейді. *ipfwadm* мен *ipchains* пәрмендері TOS-биттерімен бірге жұмыс істей алады. Екі жағдайда да, нақты белгіленген TOS-биті бар пакеттерге сәйкес келетін ереже анықталады және енгізілетін өзгерісті анықтау үші — *t* параметрі пайдаланылады.

2.3-кесте

TOS	ANDmask	XORmask	Ұсынылатын пайдалану саласы
Minimum Delay	0x01	0x10	FTP, telnet, SSH
Maximum Throughput	0x01	0x08	FTP-мәліметтер, WWW
Maximum Reliability	0x01	0x04	SNMP, DNS
Minimum Cost	0x01	0x02	NNTP, SMTP

Енгізілетін өзгерістер қосразрядты маскаларды пайдалану жолымен анықталады. Осы разрядты маскалардың біріншісі IP-пакетінің параметрлер өрісі бар AND логикалық операциясында пайдаланылады, екіншісі OR операциясында пайдаланылады. Разрядты маскалар сегіз разрядты оналтылық мәндер көмегімен анықталады;

ipfwadm мен *ipchains* бірдей синтаксис пайдаланады: — t *andmask xormask.*

Маскалар мен солардың мәндері үшін ең кеңінен қолданылатын салалар 2.3. кестесінде көрсетілген.

2.10. IP ACCOUNTING

Қазіргі таңда Интернеттің коммерциялық сервистері әлемінде желілік қосылымдарда қанша мәлімет жиналатынын және келіп түсетінін аңғарған жөн. Егер сіз интернет-провайдер болсаңыз, бұл сіздің бизнесіңіз үшін өте маңызды. Егер сіз жеткізушінің клиенті болсаңыз, онда жеткізушімен дау болған жағдайда дәлелдер келтіру үшін есеп жүргізудің маңызы зор.

Ақшалай қаражат пен есептерге еш қатысы жоқ желілік есеп жүргізудің басқа қолданылу салалары бар. Бірқатар желілік қызметтер көрсететін серверді басқарып келсеңіз, сіз үшін әрбір қызмет түрімен қанша мәлімет түрленетінін білген дұрыс болар. Осы ақпарат сізге қандай аппараттық құралдар сатып алу керек немесе қанша серверлер орындау керектігін шешуге көмектеседі.

Linux ядросы желілік трафик туралы пайдалы ақпараттың барлық түрлерін жинақтауға көмектесетін құрал болып табылады. Осы құрал *IP Accounting* деп аталады.

IP Accounting үшін ядро баптау. Linux IP Accounting-тің қасиеті Linux Firewall бағдарламалық жабдықтамамен мықты байланысқан. Мәліметтер жинақтау қажет орындар, яғни сіз Firewall-іріктеу әрекетін орындайтын орындар: желілік машина мен дейтаграмманы бағдарлауды жүзеге асыратын бағдарламалық жабдықтаманың кірісі мен шығысы.

Linux IP Accounting ті іске қосу үшін Linux ядросы сол үшін конйигурацияланғанын/конфигурацияланбағанын тексеру қажет. */proc/net/ip_acct* файлының бар екендігін біліп алу қажет. Егер де бар болса, онда IP Accounting-ті ұстанады. Болмаса, келесі опциялар үшін сіз «Y» таңдауыңыз үшін, жаңа ядро құру қажет. (ядроның 2.0 және 2.2 нұсқаларында):

Networking options ---------- >
[*] Network firewalls [*] TCP/IP networking [*] IP: accounting немесе ядроның 2.4 нұсқасында:
Networking options ---------- >
[*] Network packet filtering (replaces ipchains)

2.11. IP ACCOUNTING БАПТАУ

IP Accounting бағдарламасы IP Firewall мен нық байланыста болғандықтан, оларды баптау үшін бір-ақ бағдарлама қолданылады. Бағдарламаны іске асыру жолдарына қарай, бұл *ipfwadm* немесе *ipchains* пәрмендері арқылы жүзеге асырылады. *ipfwadm* пәрмені көмегімен IP Accounting үшін жалпы синтаксис осындай:

```
# ipfwadm -A [direction] [command] [parameters]
```

Жаңа *direction* параметрі пайда болған. Ол *in, out* немесе *both* мәндерін қабылдайды. Барлық мәндер Linux-машинасымен есептеліп шығарылады, осылайша, *in* кіріс трафикті белгілейді, *out* — шығыс трафикті белгілейді, ал *both* — екі трафик түрін бірден белгілейді.

ipchains мен *iptables* арналған жалпы синтаксис

```
# ipchains -A chain rule-specification
# iptables -A chain rule-specification
```

ipchains мен *iptables* пәрмендері ережелер анықтамаларына ұқсас бағыт анықтауға жол ашады. IP Firewall Chains бірден екі бағыт үшін ережелер баптауға жол бермейді, бірақ ескі пәрмен баптай алмаған ережелерді *forward*, пәрмендер тобында баптауға көмектеседі.

Firewall ережелері үшін пәрмендер өздерінің баламаларына өте ұқсас, тек стратегия бұл жерде қолданылмайды.

Есеп жүргізу ережелерін қосуға, енгізуге, өшіруге және шолуға болады. *ipchains* мен *iptables* пәрмендеріна келсек, барлық күші бар ережелер есеп жүргізуге арналған ережелер болып табылады және —*j* опцияны белгілемейтін кез келген пәрмен тек қана есеп жүргізу функциясын ғана орындайды.

IP-ке есеп жүргізу сипаттамасының параметрлері IP Firewall параметрлеріне ұқсас келеді.

Мекен-жайлар бойынша есеп жүргізу. IP-есебінің қалай қолданылатынын мысалмен көрсетелік. Мәселен, Virtual Brewery екі департаментіне қызмет көрсететін Linux-роутер бар делік. Оның екі Ethernet құрылғысы бар: *eth0* және *ethl,* әрбір департаментке бір-бірден, және бір құрылғы PPP — *ppp0, Groucho Marx University* университет қалашығымен тез әсер ететін бірізді байланыс орнатуға арналған.

Есепшоттар жасау үшін бөлімшелердің әрбірі пайдаланған трафиктің жалпы көлемін білу керек, және басқару мақсаттарында екі бөлімшелердің арасындағы жалпы трафигін білуі қажет.

Қолданылған мекен-жайлар мен интерфейстер 2.4. кестесінде көрсетілген.

Әрбір бөлімшенің PPP бойынша қанша мәлімет беретінін білу үшін мына ережені пайдалануға болады:

```
#          ipfwadm -A both -a -W ppp0 -S 172.16.3.0/24 -b
#          ipfwadm -A both -a -W ppp0 -S 172.16.4.0/24 -b
```

немесе:

```
# ipchains -A input -i ppp0 -d 172.16.3.0/24
# ipchains -A output -i ppp0 -s 172.16.3.0/24
# ipchains -A input -i ppp0 -d 172.16.4.0/24
# ipchains -A output -i ppp0 -s 172.16.4.0/24
```

немесе *iptables* пайдалана отырып:

```
# iptables -A FORWARD -i ppp0 -d 172.16.3.0/24
# iptables -A FORWARD -o ppp0 -s 172.16.3.0/24
# iptables -A FORWARD -i ppp0 -d 172.16.4.0/24
# iptables -A FORWARD -o ppp0 -s 172.16.4.0/24
```

2.4-кесте

Интерфейс	Мекен-жай	Тораптық маска
eth0	172.16.3.0	255.255.255.0
eth1	172.16.4.0	255.255.255.0

Әрбір ережелер тобының алғашқы бөлігі бастапқы мекен-жайы немесе мақсатты мекен-жайы 172.16.3.0/24 болып табылатын *ppp0* интерфейсі арқылы берілген барлық мәліметтердің есебін белгілейді. Мұндағы *ipfwadm* және *iptables* -дердегі ең пайдалы опция — *b.* Ережелер тобының екінші бөлігі Ethernet желісі үшін белгілеген мәндерді белгілейді.

Департаменттер арасында қандай трафик көлемі өтетінін білу үшін төмендегі ереже қолдану қажет:

```
#  ipfwadm -A both -a -S 172.16.3.0/24 -D 172.16.4.0/24 -b немесе
#  ipchains -A forward -s 172.16.3.0/24 -d 172.16.4.0/24 -b
```

немесе

```
#  iptables -A FORWARD -s 172.16.3.0/24 -d 172.16.4.0/24
#  iptables -A FORWARD -s 172.16.4.0/24 -d 172.16.3.0/24
```

Осы ережелер бойынша бір департамент желісінің шығыс мекен-жайлары мен өзге департаменттің желісіндегі кіріс мекен-жайы бар барлық пакеттер есептеп шығарылады.

Сервистер порттары бойынша есеп шығару.

PPP арқылы байланыста қандай трафик көлемі басым екендігін білу керек делік. Мысалы, FTP, SMTP мен World Wide Web хаттамалары бойынша қандай мәлімет көлемі өтетінін білу керек делік.

Сол үшін осы скрипт ережелерімен бірге пайдаланылады:

```
#!/bin/sh
#  Collect FTP, smtp and www volume statistics for data carried on our
#  PPP link usingipfwadm
#
ipfwadm -A both -a -W        ppp0 -P    tcp   -S    0/0   ftp ftp-data
ipfwadm -A both -a -W        ppp0 -P    tcp   -S    0/0   smtp
ipfwadm -A both -a -W        ppp0 -P    tcp   -S    0/0   www
```

немесе

```
#!/bin/sh
#  Collect ftp, smtp and www volume statistics for data carried on our
```

```
#  PPP link using ipchains
#
ipchains -A input -i ppp0 -p tcp -s 0/0 ftp-data:ftp
ipchains -A output -i ppp0 -p tcp -d 0/0 ftp-data:ftp ipchains -A input -i ppp0 -p tcp
-s 0/0 smtp ipchains -A output -i ppp0 -p tcp -d 0/0 smtp ipchains -A input -i ppp0 -
p tcp -s 0/0 www ipchains -A output -i ppp0 -p tcp -d 0/0 www
```

немесе

```
#!/bin/sh
#  Collect ftp, smtp and www volume statistics for data carried on our
#  PPP link using iptables.
#
iptables -A FORWARD -i ppp0 -m tcp -p tcp --sport ftp- data:ftp
iptables -A FORWARD -o ppp0 -m tcp -p tcp --dport ftp- data:ftp
iptables -A      FORWARD -i   ppp0   -m tcp    -p     tcp   --sport smtp
iptables -A      FORWARD -o   ppp0   -m tcp    -p     tcp   --dport smtp
iptables -A      FORWARD -i   ppp0   -m tcp    -p     tcp   --sport www
iptables -A      FORWARD -o   ppp0   -m tcp    -p     tcp   --dport www
```

Мұнда екі қызықты жайт бар. Біріншіден, хаттама анықталған. Ережелерде порттар белгіленген кезде, хаттаманы да анықтау қажет, себебі TCP мен UDP жеке порт тобы бар. Осы қызметтердің барлығы TCP-ге негізделгендіктен, осы хаттама анықталған болатын. Екіншіден, бір пәрменде екі сервис бөлініп отыр: *ftp* және *ftp-data*. *ipfwadm* пәрмені дара порттар, порттар ауқымдары немесе порттардың ерікті тізімдерін анықтауға жол ашады. *ipchains* пәрмені кез келген дара немесе порттар ауқымын анықтауға жол береді. *ftp-data:ftp* жазбасы «ftp-data (20) - ftp (21)» бар порттарды білдіреді, осылайша порттарды *ipchains* мен *iptables* пәрмендерге кодтауға болады. Есеп ережесінде порттар тізімінің бар екендігі кез келген портқа арналған кез келген мәліметтер осы жазбаның жалпы санына қосылатынын білдіреді. FTP екі порт, пәрмендер мен мәліметтерді пайдаланатындықтан, олар бәрі бірге FTP жалпы трафигіне қосылған. Сайып келгенде, бастапқы мекен-жай 0/0 болып белгіленген, бұл барлық мекен-жайларға сәйкес келеді және порттарды анықтау үшін *ipfwadm* және *ipchains* қажет.

Енді FTP, SMTP мен World Wide Web бойынша пайдалы трафиктің басқа хаттамалар бойынша трафикке қатынасын білу керек болып тұр. Сол үшын мына ережелер пайдаланылады:

```
# ipfwadm -A both -a -W ppp0 -P tcp -S 0/0 ftp ftp-data
smtp www
#  ipfwadm -A both -a -W ppp0 -P tcp -S 0/0 1:19 22:24 26:79 81:32767
```

Егер */etc/services*, файлы зерттелсе, онда екінші ереже ftp, ftp-data, smtp мен www нен басқа барлық порттар үшін қолданылады. Мұны *ipchains* немесе *iptables* пәрмендері үшін қалай қолдануға болады? Олар порт сипаттамасы тек бір

параметрге ғана жол береді ғой. Пайдаланушы анықтаған тізбектерді есептеп шығарған кезде Firewall ережелердегі тізбектер сияқты оңай қолдануға болады. Мына ережені қарастырайық:

#ipchains -N a-essent #ipchains -N a-noness #ipchains -A a-essent -j ACCEPT #ipchains -A a-noness -j ACCEPT
ipchains -A forward -i ppp0 -p tcp -s 0/0 ftp-data:ftp -j a-essent
ipchains -A forward -i ppp0 -p tcp -s 0/0 smtp -j a-essent
ipchains -A forward -i ppp0 -p tcp -s 0/0 www - j a-essent
ipchains -A forward -j a-noness

Мұнда пайдаланушы анықтаған екі тізбек құралады:

a-essent, мұнда пайдалы трафикке арналған мәліметтер белгіленеді және *a-noness,* мұнда қалған барлық трафик бойынша мәліметтер жинақталады. Одан кейін пайдалы сервистерге сәйкес келетін ережелер *forward* тізбегіне қосылады да, трафикті ғана есептейтін *a-essent* тізбегіне ауысу белгіленеді.

forward тізбегіндегі соңғы ереже *a-noness* тізбегіне ауысуды белгілейді, мұнда трафикті есептейтін тек бір ғана ереже бар. *a-noness* тізбегіне өтетін ережеге пайдалы серверлерден алынған кез келген пакет арқылы жетуге болмайды. Пайдалы және басқа қызметтерге арналған есептегіштерге сол тізбектер ішіндегі ережелерге қол жеткізуге болады.

Бұл таңдауға болатын тек бір-ақ тәсіл. *iptables* үшін тура осындай тәсілді орындау үшін мына ереже қолданылады:

#iptables -N a-essent #iptables -N a-noness #iptables -A a-essent -j ACCEPT #iptables -A a-noness -j ACCEPT
iptables -A FORWARD -i ppp0 -m tcp -p tcp --sport ftp- data:ftp -j a-essent
iptables -A FORWARD -i ppp0 -m tcp -p tcp --sport smtp
-j a-essent
iptables -A FORWARD -i ppp0 -m tcp -p tcp --sport www -j a-essent
iptables -A FORWARD -j a-noness

Бұл едәуір қарапайым шешім болып көрінеді. Алайда есепті қызмет түрі етуге қадам жасағанда бір шағын шарасыз мәселе туындап отыр. TCP/IP желілермен жұмыста MTU дің қызметі жоғарыда талқыланған болатын. MTU тораптық құрылғыға берілетін ең үлкен пакетті анықтайды. Пакетті бағдарлауыш алған кезде, және сол пакет оны таратуы тиіс интерфейс MTU-сынан үлкен болып қалғанда, бағдарлауыш *фрагменттеу әдісі* (fragmentation) қолданады. Бағдарлауыш үлкен пакетті интерфейс MTU-сынан үлкен емес шағын бөліктерге бөліп, сол бөліктерді таратады. Бағдарлауыш алынған пакеттердің жаңа атауларын жасайды, пакет алушы сол арқылы бастапқы пакетті қалпына келтіре алады. Өкінішке орай, фрагменттеу барысында порт мәні бірінші үзіндіден басқа барлық

үзінділер үшін жоғалтылады. Бұл IP есебінің фрагменттелген пакеттерді дұрыс есептей алмайтынын, тек бірінші үзінділері немесе фрагменттелмеген пакеттерді ғана есептей алатынын білдіреді.

Ipfwadm пәрменінде бір айла әрекет бар, ол екінші және одан кейінгі үзінділерді білмей-ақ пакеттерді есептеуге жол береді. Linux Accounting бағдарламалық жабдықтаманың бірінші нұсқасы үзінділерге есеп жасау үшін ұстап алуға болатын 0xFFFF портының өтірік нөмірін белгілеген болатын. Мына ереже бойынша екінші және одан кейінгі үзінділер белгіленеді:

```
# ipfwadm -A both -a -W ppp0 -P tcp -S 0/0 0xFFFF
```

Шешімі күрделірек бірақ нәтижесі тура сондай.

ipchains пәрменін орындау барысында келесі ережені орындау керек:

```
# ipchains -A forward -i ppp0 -p tcp -f
```

iptables үшін мына ереже келеді

```
# iptables -A FORWARD -i ppp0 -m tcp -p tcp -f
```

Осы ереже осы мәліметтер үшін бастапқы портының қандай екенін хабарламайды, бірақ мәліметтердің қаншасы үзінді болып табылатынын аңғаруға мүмкіндік береді.

2.2 ядроларында ядроны баптаған кезде осы мәселені шешетін опция табуға болады, егер Linux-машина желіге оңаша кіру нүктесі болып қызмет атқарады. Егер ядроны құрған кезде *IP: always defragment* опциясы қосылған болса, барлық пакеттерді Linux бағдарлау мен тапсыру алдында қайтадан жинақтайтын болады. Осы операция Firewall алдында орындалады, ал есеп блогы пакеттерді көре алады. Осылайша, үзінділер болмайды да, 2.4 ядроларында *forward- fragment* модулі бар netfilter құрастыру мен жүктеуге кеңес беріледі.

ICMP пакеттері бойынша есеп. ICMP хаттамасы порттардың сервистік нөмірлерін қолданбайды, сол себепті сол бойынша статистика жинақтау қиынға соғады. ICMP алуан түрлі пакеттер түрлерін пайдаланады. Солардың көпшілігінің зияны жоқ, алайда басқалары тек арнайы жағдайларда пайда болады. Кейде көп ICMP пакеттер жолдау арқылы жүйені «құлатуға» қадамдар жасалады. Бұл шабуыл *ping flooding* деп аталады. Осындай шабуылдың алдын алуда IP Firewall-ның пайдасы зор, ал IP Accounting оны кімнің істегенін табуға көмектеседі.

TCP мен UDP қарағанда, ICMP порттар пайдаланбайды. Солардың орнына ICMP хабарламалар типтері қолданылады.

ICMP хабарламаларының әрбір типін есепке алу үшін ережелер құруға болады. Сол үшін *ipfwadm* пәрменіндегі порт нөмірінің орнына ICMP хабарламасының типін анықтау қажет.

Барлық хабарлама түрлері бойынша ICMP пакеттер тарату туралы мәліметтер жинақтау үшін төмендегі ережені пайдалану қажет:

```
# ipfwadm -A both -a -P icmp -S 0/0 8
# ipfwadm -A both -a -P icmp -S 0/0 0
# ipfwadm -A both -a -P icmp -S 0/0 0xff
```

немесе *ipchains* пәрменінде

```
# ipchains -A forward -p icmp -s 0/0 8
# ipchains -A forward -p icmp -s 0/0 0
# ipchains -A forward -p icmp -s 0/0 -f
```

немесе *iptables* пәрменінде

```
# iptables -A FORWARD -m icmp -p icmp --sports echo-request
# iptables -A FORWARD -m icmp -p icmp --sports echo-reply
# iptables -A FORWARD -m icmp -p icmp -f
```

Бірінші ереже ICMP Echo Request (ping requests) пакеттер туралы ақпарат жинақтайды, екінші ереже ICMP Echo Reply (ping replies) туралы ақпарат жинақтайды. Үшінші ереже ICMP фрагменттік пакеттер туралы ақпарат жинақтайды. Осы тәсіл жоғарыда сипатталған TCP и UDP фрагменттелген пакеттерге арналған тәсілге ұқсас.

Егер ережелерде пакет көзі және (немесе) жолданушыны анықтау керек болса, пакеттердің сырттан не торап ішінен келетінін ескерген жөн.

Хаттамадар бойынша есеп.

Мысалы, трафик қандай протколдарды пайдаланатынын: TCP, UDP немесе ICMP, анықтау үшін мына ережені қолдануға болады:

```
#          ipfwadm -A both -a -W ppp0 -P tcp -D 0/0
#          ipfwadm -A both -a -W ppp0 -P udp -D 0/0
                                          # ipfwadm -A both -a -W ppp0 -P icmp -
                                          D 0/0
```

немесе

```
# ipchains -A forward -i ppp0
# ipchains -A forward -i ppp0
# ipchains -A forward -i ppp0
```

```
-p tcp -d 0/0 -p
udp -d 0/0 -p icmp
-d 0/0
```

немесе

```
# iptables -A FORWARD -i ppp0
# iptables -A FORWARD -o ppp0
# iptables -A FORWARD -i ppp0
# iptables -A FORWARD -o ppp0
# iptables -A FORWARD -i ppp0
# iptables -A FORWARD -o ppp0
```

```
-m tcp -p tcp -m tcp -
```

p tcp -m udp -p udp -m udp -p udp -m icmp -p icmp -m icmp -p icmp

Осы ережелер арқылы TCP, UDP немесе IMCP хаттамаларының арасынан дұрысын анықтау үшін *ppp0* интерфейсы арқылы трафикке талдау жасалатын болады, және тиісті есептегіштер әрбір пакет үшін өзгертілетін болады.

IP Accounting нәтижелерін қолдану.

Трафик туралы жинақталған мәліметтер мен конфигурацияланған ережелерді қарап шығу үшін Firewall баптау пәрмендері пайдаланылады.

ipfwadm, ipchains мен *iptables* пәрмендерінің ерекшелігі – жинақталған мәліметтерді өңдеу жолдарында. Сол себепті соларды жеке қарастырып өтелік.

Ipfwadm пәрменінің көмегімен мәліметтерге шолу жасау. ipfwadm пәрмені трафик туралы жинақталған мәліметтерді келесі тәсілмен қарап шығуға көмектеседі:

```
# ipfwadm -A -l IP accounting rules
pkts bytes dir prot source destination ports 9833 2345K i/o all
172.16.3.0/24 anywhere n/a 56527 33M i/o all 172.16.4.0/24 anywhere
n/a
```

Бұл әрбір бағытты ұсынатын пакеттер санын көрсетеді. Егер кеңейтілген *e* опциясы бар шығыс форматы қолданылса,
(осында көрсетілмеген, себебі тұжырымдама бір бетке сыймас еді), опциялар тізімі мен интерфейстер атаулары алынады.
Тұжырымдама көптеген өрістер түсінікті, сондықтан тек кейбіреулерін түсіндіріп кетейік:

- *dir* — ереже қолданылған бағыт. Осында күтілетін мәндер: *in, out* немесе *i/o* (екі бағытта да);
- *prot* — ережелер қолданылатын хаттама;
- *opt* — *ipfwadm* пәрменін шақырғанда қолданылатын параметрлердің кодталған формасы;
- *ifname* — ереже қолданылған интерфейс атауы;
- *ifaddress* — ереже қолданатын интерфейс мекен-жайы.

ipfwadm пәрмені әдепкі қалпы бойынша қысқартылған нұсқасында жақын тұрған мыңға (K) қарай немесе миллионға (M) қарай дөңгелектенген пакеттер есептегіштерін көрсетеді. Дөңгелектемей-ақ нақты сандарды шығару пәрменін белгілеуге болады:

```
# ipfwadm -A -l -e -x
```

ipchains көмегімен мәліметтерге шолу. — *v* параметрі белгіленбесе, *ipchains*

пәрмені есеп мәліметтерін көрсетпейді (пакеттер мен байттар есептегіштері),*:*

```
# ipchains -L -v
```

Дәл солай *ipfwadm* де — x опциясын пайдалана отырып, де пакеттер мен байттар есептегіштерін көрсетуге болады:

```
# ipchains -L -v -x
```

iptables көмегімен мәліметтерді қарап шығу. iptables пәрмені *ipchains* пәрменіне ұқсас әрекет етеді. Трафик есебінің нәтижелерін қарап шығу үшін қайтадан *v* ды пайдалану керек:

```
# iptables -L -v
```

ipchains пәрменімен тәрізді нақты мәліметтер көрсету үшін *x* ты пайдалануға болады.

Есептегіштерді қайта іске қосу. IP Accounting ке арналған есептегіштер толып кетуі мүмкін.

Осындай жағдайда солардың шынайы мәндерін анықтау қиынға соғады. Осы мәселе туындамас үшін солардың көрсетулерін мерзімді түрде хаттамалау, одан кейін келесі есеп интервалы үшін ақпарат жинау мақсатында есептегіштерді нөлге келтіру керек.

ipfwadm мен *ipchains* пәрмендері осыны оңай орындауға көмектеседі:

```
# ipfwadm -A -z
```
немесе

```
# ipchains -Z немесе
# iptables -Z
```

Есептің ешқандай мәліметтерінің жоғалмағанын қамтамасыз ету үшін тізім мен нөлдеу тұжырымын біріктіруге болады:

```
# ipfwadm -A -l -z немесе

# ipchains -L -Z немесе

# iptables -L -Z -v
```

Осы пәрмендер әуелі есептегіштерден барлық мәліметтерді көрсетеді, одан кейін есептегіштерді нөлдетіп, одан кейін есеп шығаруды басынан бастайды. Егер статистика үнемі шығарылса, тиісті пәрмендері бар скрипт жазып алып, оны *cron* арқылы шақырған жөн болар еді.

Ережелер тобын өшіру.

Соңғы бір пәрмен барлық белгіленген ережелерді өшіруге көмектеседі.

Бұл машинаға шамадан артық жүк түспес үшін ережелер тобын түбегейлі өзгерту қажет болған жағдайлар үшін өте пайдалы.

ipfwadm пәрменіндегі f параметрі белгіленген типтегі барлық ережелерді өшіріп тастайды.

Ipchains F параметрін пайдаланады, яғни:

```
# ipfwadm -A -f немесе

# ipchains -F немесе

# iptables -F
```

Бұл ережелерді бір бірден өшірмей ақ барлық ережелерді бірден өшіре салады. Назар аударыңыз, *ipchains*-те бұл операция белгіленген пайдаланушының тізбектерін өшірмей-ақ, солардан ережелерді алып тастайды.

Кіру мәліметтерінің пассивті жинақтамасы. Егер Linux-машинасы Ethernet желісіне қосылған болса, таратылған немесе қабылданған мәліметтерге ғана емес, сегменттен барлық мәліметтерге есеп шығару ережелерін қолдануға болады.

Бұл жерде машина сегменттің барлық мәліметтерін сылбыр тыңдап отырады да, оларды санап отырады.

Алдымен IP Forwarding ты Linux-машинаға жолдау қажет, бұл жерде ол алып отырған пакеттерін маршруттамауы тиіс, әйтпесе бүкіл желі «тұрып» қалады.

2.0.36 және 2.2 ядроларында бұл осылайша жасалады:

```
# echo 0 >/proc/sys/net/ipv4/ip forward
```

ifconfig пәрмені арқылы Ethernet интерфейсінде *promiscuous* режимін қосу қажет. Енді пакеттердің жергілікті желіде Linux-машинасын бағдарға қоспай-ақ пакеттердің қозғалысы туралы ақпарат жинақтауға жол беретін есеп ережелерін орнатуға болады. Назар аударыңыз: егер Linux-машина бағдарлауыш қызметін атқаратын болса, осыны жасауға тыйым салынады. Егер сіз IP Forwarding ажыратып тастасаңыз, ол бағдарлауыш қызметін атқаруды тоқтатады! Осыны тек бір физикалық желілік интерфейсі бар машинада жасаңыз.

2.12. IP MASQUERADE ЖӘНЕ NETWORK ADDRESS TRANSLATION

IP Masquerade сервисі жергілікті желіні бір компьютер арқылы үлкен сыртқы желіге қосу үшін қажетті. Бұл Firewall көмегімен желілерді қорғау қажеттілігімен байланысты, сондай-ақ жолдың толымды мекен-жайларының аса қажет болмауымен байланысты. Мысал ретінде, шағын фирманың желісін қарастырып өтелік. Оның Интернетке қосылған бір машина-шлюзы бар, қалған машиналар осы шлюз арқылы жұмыс істеуі керек.

Бірақ олардың мекен-жайлары ішкі жергілікті желіге тиесілі. IP Masquerade көмекке келеді.

Осы сервистің бір бөлігі мекен-жайлардың желі арқылы көрсетілімі болып табылады (Network Address Translation — NAT). NAT сервисі пакеттер атауларындағы желілік мекен-жайларының өзгеру үрдістерін сипаттайды.

Осы тәсіл мәселені шешу үшін ең үздік тәсіл болып табылады. Осылайша, бүкіл желі бір IP-мекен-жайы арқылы Интернет арқылы жұмыс істей алады.

IP Masquerading жекеше IP-мекен-жайын жергілікті желіде пайдалануға және сервистер мен порттарды есепке ала отырып, мекен-жайларды өзгертуді бағдарлауышқа тапсыруға жол береді. Осындай бағдарлауыш ішкі желіден пакет алған кезде, ол пакетті бағдарлауыштан алған тәрізді пакетті өзгертеді. Одан кейін пакет желіге жіберіледі. Желіден алынған жауаптар пакеттерімен де сол әрекеттер бірақ кері тәртіпте жасалады.

Жеке мекен-жайларда Интернетте қолданыла алмайтын шағын Ethernet желісі бар делік. Желіде оған Интернетке кіруге мүмкіндік беретін Linux- бағдарлауыш бар.

Желідегі автоматтандырылған жұмыс орындарының бірі (192.168.1.3) қашықтағы 209.1.106.178 компьютерге порт 8888 арқылы қосылуды ұйғарды. Автоматтандырылған жұмыс орны masquerade қызметтерінің талабы бойынша қосылуға келіп түскен осы сауалды сәйкестендіретін пакетті бағдарлауышқа жолдайды. Жолданушы компьютерінің ақпараты бойынша ол masquerade қызметтерін ұсынатын Linux-компьютері арқылы қосылған және жауап алған. Бағдарлауыш осы жауап алғаннан соң masquerade кестесінде жауап тауып алып, жолданушы мен портты кері қарай алмастырады.

Жергілікті компьютердің ақпараты бойынша, ол қашықтықтағы компьютермен тікелей жұмыс жасайды. Қашықтықтағы негізгі компьютер жергілікті компьютер туралы еш нәрсе білмейді, бірақ masquerade қызметтерін ұсынатын Linux-компьютерден желіге қосылған деп табады. Ол мына соңғы компьютердің ақпараты бойынша, осы екі компьютер бір- біріне қандай порттарда екендігін

хабарлайды да, ашық түрде бір бірімен мекен-жайлар мен порттар алмасып отырады. Сырттан бұл күрделі көрінгенімен, шынайы баптаулары қарапайымдылығымен ерекшеленеді.

Шеттегі әсерлер. IP Masquerade бірден бірнеше жанама әсер туғызады. Себебі IP Masquerade бар машина екі желінің шетінде орналасқан, әсерлер шектегі болып аталған. Masquerade бағдарлауышының артындағы желідегі компьютерлердің ешқайсысы желіде ешқашан тікелей пайда болмайды. Сол себепті, барлық компьютерлерге Интернет желісіне қосылу үшін тек бір ғана шынайы IP-мекен-жайы қажет болып тұр. Мұның теріс әсері де бар: осы компьютерлердің ешқайсысы Желіде көрінбейді, сол себепті солармен Интернет арқылы тікелей байланысуға болмайды. masquerade-желісінде көрінетін жалғыз компьютер – masquerade ты ұсынатын машина. Мұның пошта немесе FTP қызметтерін ұсыну үшін маңызы зор. Осы жайт қызметтерді masquerade-компьютер арқылы көрсету қажет екендігін анықтайды.

Екінші жайт: ішкі компьютерлер ешбір жағдайда сыртқы желіде көрінбейтіндіктен, соларды қорғауға қойылатын талаптар төмендей түседі, кей кездері шлюзде Firewall-дың қажеті жоқ. Алайда оны пайдаланған жөн, себебі бүкіл желінің сенімділігі шлюздың сенімділігімен анықталады.

Үшінші жайт: IP Masquerade желілермен жұмыстың тиімділігіне бірталай әсерін тигізеді. Машиналардың саны көп болған сайын осы құбылыс орын алады, сол себепті IP Masquerade мықты болуы керек.

Сайып келгенде, кейбір желілік сервистер masquerade арқылы мүлдем жұмыс істемейді, немесе соларды баптау үшін біраз күш жұмсауды қажет етеді. Әдетте бұл Желіге қосылу үшін қолданылатын сервистер: Direct Communications Channels (DCC), IRC, түрлі видео- и аудиокөрсетілімдер. Осы қызметтердің кейбіреулерінің пайдаланыла алмайтын модульдері бар.

Ядро мен IP Masquerade-ты баптау. IP Masquerade ты пайдалану үшін ядроны masquerade қолдай алуы үшін тиісінше құрастырылу керек. 2.2 қатарлы ядроны конфигурациялау барысында келесі параметрлерді таңдау керек:

```
Networking options ----------------- >
        [*] Network firewalls [*]
        TCP/IP networking [*] IP:
        firewalling [*] IP:
        masquerading
         ----  Protocol-specific masquerading support will be
        built as modules.
        [*] IP: ipautofw masq support [*] IP: ICMP
        masquerading
```

Назар аударыңыз, masquerade-ты қолдаудың бір бөлігіне ядро модулі ретінде қол жеткізуге болады. Бұл ядроны құрастырған кезде кәдімгі *make*

zImage ке қосымша, *make modules* пәрменін орындау қажет екендігін білдіреді.

Ядроны құрастырған кезде 2.4 қатардағы ядро нұсқа ретінде IP Masquerade-ты қолдауды енді ұсынбайды. Соның орнына желілік пакеттерді іріктеу функциясын таңдау керек.

```
Networking options ---------- >
        [M] Network packet filtering (replaces ipchains)
```

Ядроны жинастыру барысында 2.2 сериялы ядроларда хаттамалар үшін ерекше модульдер қатары жасалады. Кейбір хаттамалар бір порттағы жіберілген сауалдан басталады, одан кейін басқа компьютерде желіге қосылу уақытын күтеді. Олар әдетте masqueraded бола алмайды, себебі пакеттермен тікелей жұмысынсыз және хаттама логикасын түсінбегенше екі қосылуды да логикалық тұрғыда бір-бірімен байланыстырудың ешқандай жолы жоқ. Модульдер мынаны жасайды: олар іс жүзінде пакеттер ішіне қаратылған және masquerading ге ұстанылған хаттамалар үшін жұмыс істеуге жол береді. Осындай модульдер сондай ақ көмекші модульдер деп аталады. Ұстанылған хаттамалар 2.5 кестеде көрсетілген.

2.5 Кесте

Модуль	Хаттама
ip_masq_ftp	FTP
ip_masq_irc	IRC
ip_masq_raudio	RealAudio
ip_masq_cuseeme	CU-See-Me
ip_masq_vdolive	For VDO Live
ip_masq_quake	IdSoftware's Quake

Осы модульдерді орындау үшін оларды *insmod* пәрменін пайдалана отырып, қолмен жүктеу керек. Назар аударыңыз, осы модульдер *kerneld* домен арқылы жүктеле алмайды. Модульдердің әрқайсысы қай порттарда ол тыңдай алатынын анықтайтын параметрді қабылдайды. RealAudio модулі үшін мынаны пайдалануға болады:

```
# insmod ip masq raudio.o ports=7070,7071,7072
```

Анықталуы тиіс порттар хаттамаға тәуелді. Netfilter пакеті осыған ұқсас қызметтер атқаратын модульдерді қамтиды. Мысалы, FTP сеанстарының жұмысын қамтамасыз ету үшін *ip_conntrack_ftp* және *ip_nat_ftp. O* модульдерді пайдаланған жөн.

IP Masquerade ті баптау. IP Masquerade ережелерін баптау үшін *ipfwadm, ipchains* және *iptables* пәрмендері пайдаланылады.
Masquerade ережелері іріктеу ережелерінің арнайы классы болып табылады. Бір интерфейсте алынған пакеттердің masquerade ін қамтамасыз етуге болады, және олар басқа интерфейске жіберіледі.

Masquerade-ты баптау үшін Firewall ды жолдау ережесіне өте ұқсас, бірақ ядроға пакеттер masquerade-ын пайдалану қажеттігі туралы хабарлайтын арнайы параметрлері бар ереже жасау қажет. *ipfwadm* пәрмені *—m* опциясын пайдаланады, *ipchains* пәрмені *—j MASQ* опциясын пайдаланады, ал *iptables* пәрменінда ереженің сипаттамасына сәйкес келетін пакеттер тиісінше өзгертілуі керектігі туралы хабарлау үшін қолданылатын *j MASQUERADE* опциясы бар.

Бір мысал қарастырып өтелік. *Groucho Marx* университеті студентінің үйінде шағын Ethernet желісіне бірге қосылған бірнеше машина бар делік. Ол резервте сақталған жеке желілік мекен-жайларының бірін пайдаланады.
Желіге Интернетті пайдалануға ынталы болған басқа студенттер қосыла алады. Желіге кіру үшін қарапайым dial-up PPP қосылу жолы пайдаланылады.

Студенттер dial-up байланысын қолдау үшін және желі бағдарлауышы ретінде жұмыс істеу үшін Linux-машинаны баптайды. Оның IP-мекен-жайы модем арқылы қосылған кезде маңызды емес. Linux-бағдарлауышы IP Masquerade-ты ұстану арқылы конфигурацияланады және 192.168.1.0. жергілікті желісі үшін жеке желілік ядролардың бірін пайдаланады. Осы жерде осы желідегі компьютерлердің бірінің әдепкі қалпы бойынша белгіленген және Linux-бағдарлауышына нұсқайтын бағдары болады.

Осы конфигурацияны *ipfwadm* көмегімен іске қосу үшін осы пәрмендер іске қосу қажет:

```
# ipfwadm -F -p deny
# ipfwadm -F -a accept -m -S 192.168.1.0/24 -D 0/0 немесе ipchains пәрмені
```

көмегімен

#ipchains -P forward -j deny

ipchains -A forward -s 192.168.1.0/24 -d 0/0 - j MASQ немесе с *iptables* пәрмені

көмегімен

iptables -t nat -P POSTROUTING DROP
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE

Енді желідегі компьютерлердің қайсыбірі қашықтықтағы компьютерде сервиске қосылып көрсе, олардың пакеттері автоматты түрде Linux-бағдарлауышы арқылы masqueraded күйіне келеді. Әрбір мысалдағы бірінші ереже кез келген басқа пакетті бағдарлауға тыйым салады және қорғаныс көрсетеді.

Құрылған masquerade ережелерін қарап шығу үшін, *ipfwadm* пәрменінің —1 параметрін пайдалану қажет.

Жаңадан құрылған ережелерді бейнелеп көрсету үшін мынаны енгізу керек:

ipfwadm -F -l -e

Алынған нәтиже мынаны еске салады:

```
# ipfwadm -F -l -e
IP firewall forward rules, default policy: accept
        pkts bytes type prot opt tosa tosx ifname ifaddress 0              0 acc/m all
                        0xFF 0x00 any any
```

Мұндағы «/m» бұл masquerade ережесі екендігін көрсетеді. Ережелерді *L* опциясымен бар *ipchains* пәрмені арқылы қарап шығуға болады. *ipchains* пәрмені пайдаланылған жоғарыда көрсетілген мысалға ұқсас:

```
# ipchains -L
Chain input (policy ACCEPT):
Chain forward (policy ACCEPT):
target          prot opt          source          destination ports
MASQ            all ---------- 192.168.1.0/24 anywhere n/a
Chain output (policy ACCEPT):
```

Все правила с адресатом MASQ жолданушысына арналған барлық ережелер маскара- динг ережелері болып табылады.

Ақыр соңында дәл сол әрекетті *iptables* пәрмені арқылы орындауға болады:

```
# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt     source     destination
Chain POSTROUTING (policy DROP)
target     prot opt     source     destination
MASQUERADE all -- anywhere anywhere MASQUERADE Chain
OUTPUT (policy ACCEPT)
target     prot opt     source     destination
```

masquerade ережелері MASQUERADE жолданушымен бірге пайда болады. **IP Masquerade-ке арналған синхрондау параметрлерін орнату.** Жаңа қосылу орнатылған кезде, IP Masquerade бағдарламалық жабдықтама бір-біріне қосылған компьютерлер арасында жадыда қауымдастық құрады. Осы қауымдастықтарды кез келген уақытта */proc/net/ip_masquerade* файлында қарастыруға болады. Осы қауымдастықтар әрекетсіздік режимінде күту уақыты бар. Осы уақыт аяқталғаннан кейін байланыс жойылады.

ipfwadm пайдалана отырып, күту уақытын орнату мүмкіндігі бар.

Жалпы алғанда синтаксис осындай болады:

```
ipfwadm -M -s <tcp> <tcpfin> <udp>
```

ipchains пәрмені үшін:

```
ipchains -M -S <tcp> <tcpfin> <udp>
```

iptables пәрменін орындау арқылы әдепкі қалпы бойынша таймерлер үшін бұдан да ұзақ мәндерді пайдаланады және соларды орнатуға жол бермейді. Осы мәндердің әрқайсысы IP Masquerade бағдарламалық жабдықтама пайдаланатын таймер болып табылады. Таймерлер мен солардың пайдалану мақсаттары 2.6-кестесінде берілген.

Атаулар серверлеріне келіп түскен сауалдарды ұстап қалу.

Атау	Сипаттама
tcp	TCP сеансын күту уақыты. Задает, TCP қосылуға арналған қауымдастық жойылғанға дейін TCP- қосылу қашанға дейін активті емес болып қала беретінін анықтайды.
tcpfin	FIN нан кейін TCP күту уақыты. TCP-қосылу ажыратылғаннан кейін қауымдастық қанша уақыт бойы қала береді.
udp	UDP сеансын күту уақыты. UDP-қосылу үшін қауымдастық жойылғанға дейін UDP-қосылу активті емес болып қала береді.

Домен атауларының серверіне IP Masquerade бар желідегі машинадан келіп түскен сауалдар әрқашанда мәселелер туғызып жатты.

DNS ты masquerade ортасына бейімдетудің екі жолы бар. Компьютерлердің әрқайсысына олар дәл сол DNS пайдаланатынын және Linux-машинасы да, IP Masquerade да солардың сауалдарын DNS ке түрлендіретінін хабарлауға болады. Әйтпесе, Linux-машиасында атаулардың кэштаушы сервер орындалады және жергілікті желіде компьютерлердің әрқайсысы бапталады. Бұл жерде Linux-машинаны DNS ретінде пайдалануға болады. Мұның артықшылықтары зор, себебі DNS трафигі азайып, машина тезірек жұмыс істейді. Осы конфигурацияның кемшілігі – оның күрделілігінде.

Мекен-жайлардың желі бойынша көрсетілімі (Network Address Translation). Netfilter пакеті Network Address Translation түр түріне бейімделген. Мысалы, тек кейбір мекен-жайларды немесе мекен-жай ауқымдарын masquerade-та жасалғандай бір мекен-жайға емес, мекен-жайлар шоғырына тарататын NAT-мысалдарын қалыптастыруға болады. Бастапқы мекен-жай, мақсатты мекен-жай түрі, хаттама түрі, порт нөмірі және т.с.с стандартты анықтауышын пайдаланатын NAT ережелерін жұптар үйлесімімен бірге шығару үшін *Iptables* пәрменін іс жүзінде пайдалануға болады.

Пакеттің бастапқы мекен-жайының көрсетілімі netfilter құжаттамасында Source NAT немесе SNAT атауларымен белгілі. Пакеттің мақсатты мекен-жайының көрсетілімі Destination NAT немесе DNAT атауларымен белгілі. SNAT, DNAT және REDIRECT күрделірек ережелер жасау үшін *iptables* пәрменімен бірге пайдаланылатын жолданулары болуы мүмкін.

БАҚЫЛАУ СҰРАҚТАРЫ

1. Желілік фильтр немесе Firewall дегеніміз не?
2. Firewall-дың атқаратын қызметі қандай?
3. Firewall үшін кіріс мәліметтері қандай болып табылады?
4. Желілік іріктеудің мәні неде?
5. Firewall қандай шабуылдардан қорғалған?
6. Firewall қандай шабуылдарға төтеп бере алмайды?
7. Firewall ды іске асырудың қандай басты жолдарын білесіз?
8. Желілік іріктеу қай деңгейде жүзеге асырылады?
9. Firewall хаттамалардың қандай түрлерін іріктейді?
10. Іріктеу ережелері дегеніміз не?
11. Сіз қандай Linux IP Firewall утилиттарын білесіз?
12. IP Firewallды ұстануға арналған Linux ядросын қалай баптауға болады?

13. Ережелер мен тізбектердің өту тәртібі қалай анықталады?
14. Бағдарлау барысында қандай бастапқы оқиғалар орын алады?
15. Желіде негізгі пакеттер ағымдары қалай қалыптасады?
16. PPP катальды деңгейлі қос нүктелі хаттаманың ерекше қасиеттері қандай?
17. Іріктеу ережелерін пакетке қатысты қолданудың нәтижесінде қандай әрекеттер орындалады?
18. Пакет қозғалысының бағытына қарай ережелерді қандай санаттарға бөледі?
19. Басқа трафикке шекте қою арқылы *ipfwadm* утилитасының көмегімен ішкі желіні пайдаланушыларға Интернеттегі Web-серверіне жүгінуге қалай рұқсат беруге болады?
20. Firewall орнатылған компьютер арқылы транзитпен өтетін ереже пакеттерге таралатынын *ipfwadm* утилитасында қалай көрсетуге болады?
21. Іріктелетін пакет үшін бастапқы және соңғы жолданушы *ipfwadm* утилитасында қалайша белгіленген?
22. *ipfwadm* утилитасы желілік маскасының қандай форматын қолданады?
23. *ipfwadm* утилитасында қос бағытты ережелер қалай белгіленген?
24. *ipfwadm* утилитасы желіге қосылу үшін жолданған сауалдарды қабылдамайтын ережелерді қалай белгілей алады?
25. *ipfwadm* көмегімен өзекті ережелер тобын қалай қарап шығуға болады?
26. Орнатылған желілік қалқаны бар компьютерде қанша желілік интерфейс болу керек және олар не үшін болу керек?
27. *Ipfwadm*-те желілік іріктеудің қандай стратегиялары іске асырылған?
28. *ipfwadm* мен салыстырғанда IP Firewall Chains де қандай жаңа нәрселер пайда болған*?*
29. *ipchains* ты пайдаланудың қандай жолдары бар*?*
30. *ipchains* ке жаңа тізбекті қалай қосуға болады*?*
31. *ipchains* те қандай жаңа стратегиялар пайда болған*?*
32. Ереженің шарттарын орындайтын пакетпен не істеу керектігін *ipchanes* қалай көрсетеді?
33. *ipchains* те өзекті ережелерді қалай қарап шығуға болады?
34. *ipchans* не арқылы пакет фильтрінің өнімділігін айтарлықтай арттыруға жол ашады?
35. *ipchans* те пайдаланушы анықтаған тізбекті қалай бекітуге болады?
36. *ipchains* қолдау скриптілері дегеніміз не және олардың атқаратын қызметтері қандай?
37. Netfilter пакеті қандай мәселелерді шешуге көмектескен?
38. Netfilter ді қалай *ipchanes* утилитін эмульдеткізе алуға болады?
39. Netfilter қандай пәрмендер орындай алады?
40. Netfilter қандай кеңейтілім түрлерін ұстанады?
41. Netfilter (TOS) қызмет көрсету түрінің биттерін қалай өңдейді?
42. IP Accounting тің қолданылу саласын қандай?
43. IP Accounting мекен-жайларына қалай есеп жүргізіледі?
44. IP Accounting-те сервис порттары бойынша есеп қалай жүргізіледі?
45. IP Accounting-те хаттамалар бойынша есеп қалай жүрігізіледі?
46. Есеп жүргізу барысында алынған мәліметтерді IP Accounting-те қалай қарап шығуға болады?

47. IP Accounting-те есептегіштерді қалай қайта қосуға болады?
48. Есеп ережелерінің топтамаларын қалай өшіруге болады?
49. Мекен-жайлардың желідегі көрсетілімі не үшін қажет?
50. IP Masquerading қандай әрекеттер орындауға жол ашады?
51. Шеттегі әсерлер дегеніміз не?
52. IP Masquerade қалай бапталады?
53. IP Masquerade үшін синхрондау параметрлері қалай белгіленеді?

КОМПЬЮТЕРЛІК ЖҮЙЕЛЕРДІ ӘКІМШІЛЕНДІРУ ЖӘНЕ ҚЫЗМЕТ КӨРСЕТУ

II

ТАРАУ

3 бөлім. ақпаратты қауіпсіз тарату үшін сервер мен жұмыс станцияларын баптау
4 бөлім. жергілікті және ауқымды желілерге қол жетімділігін ұйымдастыру.
5-бөлім. Web-сервер, файлдық сервер, пошталық сервер, sQL-серверді пайдалануға сүйемелдеу және бақылау

3 тарау

АҚПАРАТТЫ ҚАУІПСІЗ ТАРАТУ ҮШІН СЕРВЕР МЕН ЖҰМЫС СТАНЦИЯЛАРЫН БАПТАУ

3.1. DCHP SERVER ҚЫЗМЕТІН БАПТАУ

Тораптар динамикалық конфигурациясының хаттамасы (Dynamic Host Configuration Protocol — DHCP) TCP/IP желілерінде конфигурациялық ақпаратты желілік тораптарға берілуін сипаттайды. IP-мекенжайларын автоматты бөлу (оның ішінде қайтадан) және қосымша конфигурациялық параметрлерді (опцияларды) таратуға мүмкіндік бере отырып, DHCP аса ескі BOOTP (Bootstrap Protocol) хаттамасына негізделеді.

DHCP желі тораптарына конфигурациялық параметрлерді береді. DHCP екі құрамдас бөліктен: DHCP-серверден шыққан желі тораптары үшін ерекше конфигурациялық параметрлерді жеткізуге арналған хаттамадан және желілік мекенжайлардың жалпы кеңістігінен шыққан желілік мекенжайларды белгілеу тетігінен тұрады.

DHCP клиент-сервер үлгісі бойынша жасалған және бұнда белгіленген DHCP-серверлер желілік мекенжайларды ерекшелейді де, тиісті конфигурациялық параметрлерді динамикалық бапталушы желі тораптарына жеткізеді.

Желі торабы DHCP-сервер рөлінде шықпауы тиіс, егер де бұл айқын көрсетілген болмаса. Бұндай жағдайда DHCP алуан түрлі жабдықталуы мен іске асырылуы желінің сенімді конфигурациясының құрылуына жол бермеуі мүмкін. Мысалы, IP хаттамасы нақты бір бағдарламаны орындау шеңберінде көптеген параметрлерді талап етеді. IP-хаттамасы әр түрлі жабдықтарда қолданылуы мүмкін болған соң, конфигурация параметрлерінің мәні алдын ала табылып, үнсіз келісім бойынша орынды мағына беруі мүмкін емес.

Белгіленген мекенжайларды тарату сызбасы желідегі қосарланған мекенжайлардан шыққан қорғау тетігіне тәуелді болады.

DHCP IP-мекенжайларын тағайындайтын 3 тетікті ұстайды. Автоматты белгілеген кезде DHCP клиентке тұрақты IP-мекенжай тағайындайды. Динамикалық белгілеген кезде DHCP белгілі уақыт кезеңіне (немесе клиент IP-мекенжайды айқын түрде босатқан сәтке дейін) клиентке IP-мекенжай тағайындайды.

Қолмен белгілеген кезде клиенттің IP-мекенжайы желі әкімшісімен тағайындалады да, DHCP клиентке тек осы мекенжайды хабарлау үшін пайдаланылады. Көбінесе желіде жоғарыда баяндалған мекенжайлар белгілейтін тетіктердің бір немесе бірнешеуі пайдаланылады.

Үш тетіктің ішінен динамикалық белгілеу автоматты түрде

мекенжайды қайтадан пайдалануға рұқсат ететін жалғыз тетік болып есептеледі, егер де ол бұдан бұрын тағайындалған клиентке ендігәрі керек болмаса. Осылайша, динамикалық белгілеу желіге уақытша немесе IP-мекенжайлардың шектелген ауқымын тарату үшін қосылатын клиенттердің мекенжайларын тағайындаған кезде аса пайдалы болып табылады. Сондай-ақ динамикалық белгілеу IP мекенжайларды шалғайдағы клинттерден автоматты түрде босату үшін DHCP-сервердің билігіндегі IP-мекенжай ауқымының мөлшері жеткіліксіз болған кезде желіге тұрақты қосылып отыратын жаңа клиентке IP-мекенжайды тағайындауға да ыңғайлы болып табылады.

Мекенжайларды қолмен белгілеу DHCP тетіктерін пайдаланбай IP мекенжайлардың басым көпшілігін қолмен белгілейтін орталардағы желі тораптарына желіні орнықтыру кезінде DHCP ықтимал қателерді жібермеуге мүмкіндік береді.

DHCP хабарламалар пішімі хаттамалар сәйкестігін және соның салдарынан BOOTP-клиенттердің DHCP-серверлерімен жұмыс жасау қабілетін қамтамасыз ету үшін BOOTP хабарлама пішіміне негізделген.

Клиент пен сервердің өзара әрекеті. Клиент пен сервердің қатынасу процесі мынадай операциялардан тұрады:

1. Клиент сервердің жергілікті физикалық бағыңқы желісіне DHCPDISCOVER типті тарату ауқымы кең хабарлама жібереді. DHCPDISCOVER хабарламасы клиентпен сұратылған конфигурациялық параметрлер опциялары мен мәндерінен тұруы мүмкін. BOOTP Relay агенттері осы хабарламаларды DHCP-серверге береді, егер де ол басқа бағыңқы желіде болса.
2. Әр сервер қолжетімді IP-мекенжайдан тұратын DHCPOFFER хабарламасымен жауап береді. Сондағы сервер мекенжайлар таралымын орындау жылдамдығын арттыруына қарамастан осы мекенжайды резервте сақтамайды. IP-мекенжайды белгілеген кезде сервер белгіленген IP-мекенжай желіде қолданылмайтынын міндетті түрде тексереді. Мысалы, сервер ICMP эхо-пакетіне сұрау салу арқылы осы IP-мекенжайдың қолданылуын тексере алады. DHCP-сервердің жүзеге асырылуына байланысты IP-мекенжайдың қолданылуын осылайша тексеретін командасы өшірулі болуы мүмкін. Қажетіне қарай DHCP-сервер BOOTP Relay серверін пайдалана отырып, клиентке DHCPOFFER хабарламасын жібереді.
3. Клиент бір немесе бірнеше DHCP-серверден бір немесе бірнеше DHCPOFFER хабарлама алады. Клиент әр түрлі серверлерден көптеген жауаптарды алу үшін күте тұруына болады. Бұдан кейін клиент жауапта келген параметрлерге байланысты DHCPOFFER жауаптарының бірін таңдайды. Клиент DHCPREQUEST тарату ауқымы кең хабарламаны жолдайды. Оның құрамына DHCP-клиентпен қай сервердің жауабы таңдалғанын көрсету үшін *'server identifier*(ағылш. — сервер идентификаторы)опциясы енгізілуі тиіс.

Сонымен қатар сұратымда қалаулы конфигурация параметрлері сипатталатын басқа да опциялар қатысуы мүмкін. *'requested IP address* өрісі DHCPOFFER хабарламасының *'yiaddr'* өрісінен түскен мәнде белгіленуі тиіс. Осы DHCPREQUEST хабарламасы кең таралып жолданады да, сол BOOTP Relay арқылы келеді.

4. DHCP-серверлер клиент атынан жолданған DHCPREQUEST хабарламаларды алады. Клиентпен таңдалмаған серверлер осы хабарламаны клиент оған ұсынылған қосу параметрлерін қабыл алмағаны туралы хабарлама ретінде пайдаланады. Клиентпен таңдалған сервер өзінің тұрақты сақтау орнына желі торабы мен IP-мекенжай байланысын жазып алады да, клиентке осы желі торабының конфигурациялық параметрлерінен тұратын DHCPACK хабарламасымен жауап береді. Клиент идентификаторының комбинациясы *('client identifier'*или *'chaddr')* және оған бөлінген IP-мекенжайлар клиент пен серверді бұдан әрі хабарламаларда еске алу үшін жалдайтын бірегей идентификаторы (lease) болып табылады. DHCPACK хабарламаларында жолданатын конфигурация параметрлерінің бірі де DHCPOFFER хабарламаларында бұдан бұрын жолданған параметрлерге қайшы келмеуі тиіс. Осы сәтте серверге белгіленген IP-мекенжайды тексеруге талап қойылмайды, себебі тексеру бұдан бұрын жүргізілген. DHCPACK хабарламасының *'yiaddr'* өрісінде осы мекенжай орналастырылады.

   Егер DHCP-сервер түрлі себептерге байланысты DHCPREQUEST сұрауын қанағаттандыра алмаса (мысалы, егер сұратылған IP-мекенжай әлдеқашан белгіленген болып шықса), сервер DHCPNAK хабарламасымен жауап береді.

   Сервер DHCPOFFER хабарламаларына жіберілген IP-мекенжайларды қол жетпейтін деп белгілеуі мүмкін. Бұл жағдайда сервер мекенжайдан бұндай белгіні алып тастауы қажет, егер де DHCPOFFER-ге клиенттен жауап келмеген болса.

5. Клиент конфигурациялық параметрлері бар DHCPACK хабарламасын алады. Клиент хабарламада келген конфигурациялық параметрлерді тексереді де, осы хабарламада келген мекенжайды жалдау уақыты туралы ақпаратты сақтайды. Осы сәттен бастап клиент конфигурацияланған болып саналады. Егер клиент қандай да бір қатені анықтаса (мысалы, IP-мекенжай пайдаланылуда), ол серверге DHCPDECLINE хабарлама жолдайды да, баптау процесін қайтадан бастайды. Клиент трафиктің шамадан тыс асып кетпеуі үшін қайтадан конфигурацияны бастағанға дейін аз дегенде 10с тоқтай тұруы керек.

Егер клиент DHCPNAK хабарламасын алса, ол конфигурацияны тағы қайтадан бастайды.

Егер клиент не DHCPNAK, не DHCPACK алмаса, ол тосу уақыты біткеннен кейін DHCPREQUEST хабарламаны қайтадан жібереді. Клиент DHCPREQUEST хабарламаны жіберу әрекетінің орынды санын таңдауы қажет. Бір жағынан, сервер осы хабарламаны алғанына көзі жетсе, екінші жағынан, клиент конфигурацияны тосып, көп уақытын кетірмейді.

6. Клиент IP-мекенжай ендігәрі талап етілмейтіні және оны басқа желілік тораптармен белгілеуге болатыны туралы хабарлау үшін серверге DHCPRELEASE хабарламасын жолдай алады. Жалға алынған IP-мекенжай DHCPRELEASE хабарламасында *'client identifier'* немесе *'chaddr'* өрісі және оған берілген желілік мекенжаймен сәйкестендіріледі.

Бұдан бұрын берілген IP-мекенжайды қайтадан пайдалану. Егер клиентке бұдан бұрын берілген IP-мекенжай белгілі болса, ол мекенжай алудың қысқартылған процедурасын пайдалана отырып, оны қайтадан қолдануға сұрау сала алады.

1. Клиент тарату ауқымы кең DHCPREQUEST хабарламаны оның жергілікті физикалық бағыңқы желісіне жолдайды. Хабарламада *'requested IP address'* опциясы ретінде IP-мекенжай болады. BOOTP Relay сервері басқа бағыңқы желілердегі DHCP-серверлерге сұрау береді (егер бұл қажет болса). Егер клиент сұралған мекенжайды алған кезде бұдан бұрын *'client identifier'* пайдаланған болса, ол осы опцияны DHCPRE- QUEST хабарламасында да көрсетеді.
2. Конфигурациялық параметрлері белгілі серверлер клиентке DHCPACK хабарламасы арқылы жауап береді. Сервер таңдалған IP-мекенжайды пайдаланылуына тексеру жүргізбейді. Бұны клиент орындайды.

Егер клиент сұранысы түзу болмаса (мысалы, клиент басқа бағыңқы желіге ауыстырылған), сервер оған DHCPNAK хабарламасымен жауап беруі қажет.

3. Клиент конфигурациялық параметрлері бар DHCPACK хабарламасын алады. Клиент параметрлер түзулігіне соңғы тексеру жүргізеді де, хабарламада келген жалдау уақытын жадында ұстайды. Осы сәттен бастап клиент бапталған болып есептеледі.

   Егер клиент DHCPACK келген мекенжайдың баяғыдан пайдаланылатына көзі жетсе, ол серверге DHCPDECLINE хабарламасымен жауап береді де, жаңа IP-мекенжайға сұрау салу үшін баптау процесін қайтадан жаңартады.

   Егер клиент DHCPNAK хабарламасын алса, ол бұдан бұрын сақталған IP-мекенжайды ендігәрі пайдалана алмайды.

   Клиент жаңа мекенжайды алу процедурасын тағы да жүргізуі тиіс.

4. Клиент серверге DHCPRELESE хабарламасын жіберу арқылы берілген IP-мекенжайды босатуды да айқын сұрай алады.

   DHCP-клиент пен DHCP-сервер айырбастай алатын хабарламалардың толық тізіміне мыналар кіреді:

   1) DHCPDISCOVER — клиент оның желісіндегі барлық қолжетімді DHCP-серверлерді табу үшін осы хабарламаны жолдайды;
   2) DHCPOFFER — сервер конфигурациялық параметрлерді ұсына отырып, осы хабарламаны клиентке жолдайды;
   3) DHCPREQUEST — клиент серверлерге хабарламаны жолдайды:
      - бір DHCP серверінен ұсынылған параметрлерді сұрау үшін;
      - басқа DHCP серверлер параметрлерінің ұсынысынан бас тарту үшін;

- берілген мекенжайға жалдау уақытын ұзарту үшін;

4) DHCPACK — сервер конфигурациялық параметрлер мен берілген IP-мекенжайымен хабарламаны жолдайды;
5) DHCPNAK — сервер клиентпен сұратылған параметрлер сервермен қаралмай қайтарылғаны туралы хабарлама жібереді;
6) DHCPDECLINE — клиент берілген IP-мекенжай әлдеқашан пайдаланылатыны және клиент үшін тиімді екенін көрсете отырып, хабарлама жібереді;
7) DHCPRELEASE — клиент оған берілген IP-мекенжайдың босатылуын нақты сұрау үшін хабарлама жолдайды;
8) DHCPINFORM — баяғыдан конфигурацияланған кезде клиент серверден кейбір параметрлерді сұрайды.

Алу процесі. DHCP көмегімен IP-мекенжайды бөлу процесіне мысал қарастырайық. Журналды мысал етіп көрсеткенде DHCPDISCOVER — DHCPOFFER — DHCPREQUEST — DHCPACK реттілігі бойынша хабарламаның жіберілуі жақсы көрсетілген:

2014-07-04T11:27:09.969169+04:00 server dhcpd: DHCPDISCOVER from 08:00:27:44:99:fc via enp0s8 2014-07-04T11:27:10.970987+04:00 server dhcpd: DHCPOFFER on 192.168.0.100 to 08:00:27:44:99:fc (client) via enp0s8 2014-07-04T11:27:11.049039+04:00 server dhcpd: DHCPREQUEST for 192.168.0.100 (192.168.0.1) from 08:00:27:44:99:fc (client) via enp0s8 2014-07-04T11:27:11.049039+04:00 server dhcpd: DHCPACK on 192.168.0.100 to 08:00:27:44:99:fc (client) via enp0s8

Келтірілген журналдың үзіндісі DHCP серверінен алып тасталған. Бұнда *enp0s8* — DHCP- сервер белсене қатысатын сервердің желілік интерфейсі; *192.168.0.100* — берілген IP-мекенжай; *08:00:27:44:99:fc* — DHCP клиенттің (конфигурациялық желелік торабының) MAC-мекенжайы; *client*— клиенттің желілік атауы. DHCP сервердің атауы — *formicae.*

Клиент пен сервер арасында осы уақыт аралығында берілетін пакеттерді қарастырайық. Пакеттер *tcpdump — vvv* командасының көмегімен алып тасталған.

11:27:09.969169 IP (tos 0x10, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 328)
0.0.0.0.bootpc > 255.255.255.255.bootps: [udp sum ok] BOOTP/DHCP, Request from 08:00:27:44:99:fc (oui Unknown), length 300, xid 0xad5ad501, Flags [none] (0x0000)
Client-Ethernet-Address 08:00:27:44:99:fc (oui Unknown)
Vendor-rfc1048 Extensions Magic Cookie 0x63825363
DHCP-Message Option 53, length 1: Discover Client-ID Option 61, length

7: ether 08:00:27:44:99:fc
Vendor-Class Option 60, length 12: "dhcpcd
3.2.3"
Hostname Option 12, length 6: "client" Parameter-Request Option 55, length 1:
Domain-Name-Server
END Option 255, length 0
22

Бұнда DHCPDISCOVER хабарламасы (DHCP-Message өрісі тарату ауқымы кең 255.255.255.255. bootps мекенжайы бойынша) берілгені көрсетілген . Осы хабарламаға сервер DHCPOF- FER хабарламасымен жауап береді:

11:27:09.969169 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.100 tell server. mysite.org, length 28
11:27:10.965959 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.100 tell server. mysite.org, length 28
11:27:10.970787 IP (tos 0x10, ttl 128, id 0, offset 0, flags [none], proto UDP (17), length 328)
server. mysite.org.bootps > 192.168.0.100.bootpc: [udp sum ok] BOOTP/DHCP, Reply, length 300, xid 0xad5ad501, Flags [none] (0x0000)
Your-IP 192.168.0.100
Client-Ethernet-Address 08:00:27:44:99:fc (oui Unknown)
Vendor-rfc1048 Extensions Magic Cookie 0x63825363 DHCP-Message Option 53, length 1: Offer Server-ID Option 54, length 4: server.mysite.
org
Lease-Time Option 51, length 4: 14400 Domain-Name-Server Option 6, length 4: server. mysite.org
Subnet-Mask Option 1, length 4: 255.255.255.0
END Option 255, length 0
PAD Option 0, length 0, occurs 32

DHCPOFFER хабарламасын алып, клиент серверге DHCPREQUEST хабарламасында IP-мекенжайына сұрау салады:

11:27:10.971575 IP (tos 0x10, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 344)
0.0.0.0.bootpc > 255.255.255.255.bootps: [udp sum ok] BOOTP/DHCP, Request from 08:00:27:44:99:fc (oui Unknown), length 316, xid 0xad5ad501, secs 1, Flags [none] (0x0000)
Client-Ethernet-Address 08:00:27:44:99:fc (oui Unknown)
Vendor-rfc1048 Extensions Magic Cookie 0x63825363
DHCP-Message Option 53, length 1: Request MSZ Option 57, length 2: 1500 Client-ID Option 61, length 7: ether 08:00:27:44:99:fc
Vendor-Class Option 60, length 12: "dhcpcd

3.2.3"
Requested-IPOption 50, length 4: 192.168.0.100 Server-ID Option 54, length 4: server. mysite.
org
Hostname Option 12, length 6: "client" Parameter-Request Option 55, length 23:
RN, RB, Subnet-Mask, BR Classless-Static-Route, Static-Route, Default-Gateway, Hostname
Option 119, Domain-Name, Domain-Name-Server,
YD
YS, NTP, MTU, RP
Option 120, LPR-Server, LOG, Netbios-Name-Server
WDD, Netbios-Node, Netbios-Scope END Option 255, length 0

Ақыр соңында, сервер клиенттің сұрауы қанағаттандырылғаны жайында оған жауап қайтарады:

11:27:11.049039 IP (tos 0x10, ttl 128, id 0, offset 0, flags [none], proto UDP (17), length 328)
server.mysite.org.bootps > 192.168.0.100.bootpc: [udp sum ok] BOOTP/DHCP, Reply, length 300, xid 0xad5ad501, secs 1, Flags [none] (0x0000)
Your-IP 192.168.0.100
Client-Ethernet-Address 08:00:27:44:99:fc (oui Unknown)
Vendor-rfc1048 Extensions
Magic Cookie 0x63825363
DHCP-Message Option 53, length 1: ACK
Server-ID Option 54, length 4: server.mysite.org
Lease-Time Option 51, length 4: 14400
Subnet-Mask Option 1, length 4: 255.255.255.0
Default-Gateway Option 3, length 4: server. mysite.org
T119 Option 119, length 12: 107837811,1769235715,1869768448
Domain-Name Option 15, length 10: "mysite.org" Domain-Name-Server Option 6, length 4: server. mysite.org
END Option 255, length 0

Мекенжайлардың ауқымдарын жасау. DHCP-серверлердің қаралуы ICS DHCP мысалында жүргізіледі. Сервер мен клиент жүйелік журналдарының *tcpdump* көмегімен DHCP-сервер жұмысын ретке келтіріп, оған диагностика жүргізуге болады.

DHCP-сервердің конфигурациясы бір */etc/ dhcpd. Conf* файлында болады, егер де басқасы орнату кезінде көрсетілген болмаса. Сервердің қарапайым конфигурациясын қарастырайық: server:~ # cat /etc/dhcpd. conf option domain-name "mysite.org"; option domain-name-servers 192.168.0.1; option domain-search

```
"mysite.org"; default-lease-time 14400; authoritative;
subnet 192.168.0.0 netmask 255.255.255.0 { range 192.168.0.100 192.168.0.200; option
        routers 192.168.0.1; default-lease-time 14400; max-lease-time 172800;
}
```

Файлдың басында барлық DHCP-клиенттер үшін баптаудың жалпы параметрлерін көрсететін опциялар орналасады. Бұндай опцияларға мыналар жатады:

- *domain-name*— DNS-доменнің атауы, оған барлық тораптар тиесілі;
- *domain-name-servers* - DHCP клиенттеріне қолжетімді DNS-серверлер;
- *domain-search*— желілік атауды іздеу үшін домен жұрнақтарының тізімі.

Сірә, осы үш опция DNS рұқсатын баптауға ғана жауап береді.

default-lease-time өрнегі үнсіз келісім бойынша пайдаланылатын IP-мекенжайды бөлу (жалдау) уақытын көрсетеді, яғни егер клиент жалдаудың айрықша уақытын (секундтармен өлшенеді) сұрамаса. Осылайша, келтірілген мысалда клиентке мекенжай үнсіз келісім бойынша 4 сағатқа жалға берілетін болады. Қандай да бір клиентпен IP-мекенжайдың пайдаланылу уақыты осындай мәнмен шектелмейді. Ол тек жалдау қашан аяқталатынына уақыт белгілейді және клиент оны сұрау салу арқылы ұзарта алады.

Бұдан кейін бағыңқы желілер хабарланады. Жалпы алғанда DHCP-сервер, мысалы, BOOTP Relay-серверлерді пайдалану арқылы немесе жай ғана түрлі желілік интерфейстерде бірнеше бағыңқы желілерге қызмет көрсете алады. Бағыңқы желілер қарапайым түрде бағыңқы желі қалқасымен сәйкестендіріледі.

Бағыңқы желі жарияланымы ішінде осы бағыңқы желі үшін ерекше болып табылатын опциялар мен баптаулар болуы мүмкін. Мысал ретінде маршруттау (option router) және жалдау уақытының (default-lease-time и max-lease-time) баптаулары келтірілген.

Берілетін мекенжайлардың ауқымын жариялау (range) бағыңқы желідегі негізгі параметрлердің бірі болып табылады. Бағыңқы желі сипаттамасында кем дегенде бір ауқым болуы қажет, егер де бағыңқы желіде мекенжайларды автоматты түрде бөлу жүзеге асырылуы керек болса. *range* жарияланымының мынадай синтаксисі бар:

```
range [ dynamic-bootp ] low-address [ high-address];
```

Ауқымның жарияланымы бөлуге қол жетімді төменгі *(low-address)* және жоғарғы *(high-address)* мекенжайларды көрсетеді. Көрсетілген мекенжайлар толықтай ауқым көрсетілген бағыңқы желілер шеңберінде болуы қажет. *dynamic-bootp* жалауы DHCP клиенттерімен қатар BOOTP клиенттерінің жұмысын қамтамасыз ету үшін орнатылады. Егер ауқымның оң жақ шекарасы *(high-address)* көрсетілмесе, ауқым жалғыз *low-address* IP-мекенжайынан тұратын болып саналады.

Ағымдағы берілген мекенжай осы ауқымнан тыс болып шығуы үшін

берілген мекенжайлар ауқымын өзгертіп көрейік:

```
server:/etc # cat /etc/dhcpd. conf option domain-name
"mysite.org"; option domain-name-servers 192.168.0.1; option
domain-search "mysite.org"; default-lease-time 14400;
authoritative;
subnet 192.168.0.0 netmask255.255.255.0 { range 192.168.0.150
        192.168.0.200; option routers 192.168.0.1; default-lease-
        time 14400; max-lease-time 172800;
}
```

Ғылыми тәжірибе ретінде DHCP клиенттің доменін желілік интерфейсте қолмен іске қосып тоқтатып көрейік:

```
ifconfig enp0s3 up dhcpcd
enp0s3
```

DHCP-клиентті тоқтату мақсатында оған аяқталу сигналын жіберуге болады:

```
killall dhcpcd
```

Бұдан әрі пакеттің толық құрылымын қарамай, тек жүйелік журналдың жазбасын келтіреміз *(/var/log/messages).*

DHCP-клиентті қайтадан іске қосқаннан кейін жүйелік журналда келесі көрінеді:

```
2014-07-04T11:42:12.810446+04:00 server dhcpd: All rights reserved.
2014-07-04T11:42:12.810959+04:00 server dhcpd: For info, please visit https://www.
isc.org/software/dhcp/ 2014-07-04T11:42:12.812893+04:00 server dhcpd: Not searching
LDAP since ldap-server, ldap-port and ldap- base-dn were not specified in the config file
2014-07-04T11:42:12.813423+04:00 server dhcpd: lease 192.168.0.100: no subnet.
2014-07-04T11:42:12.813924+04:00 server dhcpd: Wrote 0 leases to leases file.
2014-07-04T11:42:12.894512+04:00 server dhcpd: Listening on
LPF/enp0s8/08:00:27:cb:f9:9f/192.168.0.0 /24
2014-07-04T11:42:12.895572+04:00 server dhcpd: Sending on
LPF/enp0s8/08:00:27:cb:f9:9f/192.168.0.0/24 2014-07-04T11:42:12.896393+04:00
server dhcpd: Sending on Socket/fallback/fallback-net
2014-07-04T11:42:12.900582+04:00 server dhcpd[6204]: Starting ISC DHCPv4 4. x
Server [chroot]..done 2014-07-04T11:42:12.901350+04:00 server systemd[1]: Started
LSB: ISC DHCP 4.x Server.
```

«lease 192.168.0.100: no subnet» сөйлемшесі DHCP-сервердің деректер қорында 192.168.0.100 мекенжайын жалдау туралы жазба бар екенін білдіреді, алайда ол ағымдағы сервер конфигурациясына кіргізілмейді.

Клиентке dhcpcd -n enp0s3 жалдауды жаңарту үшін сұрау салу нәтижесінде клиент серверге оны ұзарту жайында мерзімдік сұраулар жолдай

бастайды(DHCPREQUEST).

11:48:36.941846 IP (tos 0x0, ttl 64, id 46894, offset 0, flags [DF], proto UDP (17), length 332)
192.168.0.100.bootpc > server. mysite.org. bootps: [udp sum ok]
BOOTP/DHCP, Request from 08:00:27:44:99:fc (oui Unknown), length 304, xid 0x8084bc35, Flags [none] (0x0000)
Client-IP 192.168.0.100
Client-Ethernet-Address 08:00:27:44:99:fc (oui Unknown)
Vendor-rfc1048 Extensions Magic Cookie 0x63825363
DHCP-Message Option 53, length 1: Request MSZ Option 57, length 2: 1500 Client-ID Option 61, length 7: ether 08:00:27:44:99:fc
Vendor-Class Option 60, length 12: "dhcpcd 3.2.3"
Hostname Option 12, length 6: "client" Parameter-Request Option 55, length 23:
RN, RB, Subnet-Mask, BR Classless-Static-Route, Static-Route, Default-Gateway, Hostname
Option 119, Domain-Name, Domain-Name-Server, YD
YS, NTP, MTU, RP
Option 120, LPR-Server, LOG, Netbios-Name-Server
WDD, Netbios-Node, Netbios-Scope END Option 255, length 0

Осы уақытта сервердің жүйелік журналында мына хабарламаны көруге болады:

2014-07-04T11:48:02.662351+04:00 server dhcpd: DHCPREQUEST for 192.168.0.100 from 08:00:27:44:99:fc via enp0s8: unknown lease 192.168.0.100.

Мекенжайды босатуға әрекеттеніп, қайтадан сұрау салу сияқты әрекеттер жағдайды түзеуге көмектеседі. Келесі командаларды жүргізу арқылы жағдайды түзеуге болады:
dhcpcd -k enp0s3 dhcpcd
-n enp0s3

Сервердің жүйелік журналында мынаны көруге болады:

2014-07-04T11:52:48.077110+04:00 server dhcpd: DH- CPRELEASE of 192.168.0.100 from 08:00:27:44:99:fc via enp0s8 (not found)
2014-07-04T11:53:10.408500+04:00 server dhcpd: DHCPDISCOVER from 08:00:27:44:99:fc via enp0s8 2014-07-04T11:53:11.410211+04:00 server dhcpd: DHCPOFFER on 192.168.0.150 to 08:00:27:44:99:fc (client) via enp0s8
2014-07-04T11:53:11.423796+04:00 server dhcpd: DHCPREQUEST for 192.168.0.150

(192.168.0.1) from 08:00:27:44:99:fc (client) via enp0s8 2014-07-04T11:53:11.423796+04:00 server dhcpd: DHC- PACK on 192.168.0.150 to 08:00:27:44:99:fc (client) via enp0s8

Яғни клиенттің мекенжайды жаңа ауқымнан алуы сәтті өтті. Клиент серверге DHCPREQUEST хабарламасын мекенжайды жалдау мерзімі аяқталғанға дейін жібере берерін есте сақтаңыздар. IP-мекенжайды жалдау мерзімін өте аз уақыт аралығына (5 немесе 10 минутқа дейін) өзгертуді DHCP клиенттер жаңа баптауға серпінді өтуі үшін пайдалана алады.

Берілген IP-мекенжайларды концигурациялау. Берілген IP-мекенжайлар (немесе DHCP терминологиясы бойынша – IP-мекенжайларды қолмен бөлу) желілік тораптарды сәйкестендіретін ақпаратты көрсете отырып, оларды тікелей санап шығуымен анықталады. Бұл *host* өрнегінің көмегімен орындалады:

```
host hostname {
        [ parameters ]
        [ declarations ]
}
```

host (желілік торап) өрнегі бір DHCP клиент үшін параметрлер қызметінің аясын анықтайды. Соның ішінде сұралған IP-мекенжайды клиентке бөлу мүмкіндігін ұсынады.

Қалауынша, бір клиентті әр түрлі бағыңқы желілерде баптау мүмкіндігі үшін бір түйінге бірнеше статикалық IP-мекенжайды көрсетуге немесе керісінше, әр түрлі бағыңқы желілерде әр түрлі *host* өрнегінде бір желілік торапты көрсетуге мүмкіндік беріледі.

hostname өрісі клиентті сәйкестендіру үшін пайдаланылуы тиіс. Егер *hostname* опциясы сервермен көрсетілмесе, *host* өрнегіндегі *hostname* жолының мәні пайдаланылады.

DHCP-сервердің көрсетілген конфигурациясына статикалық IP-мекенжайды қосып көрейік:

```
option domain-name "mysite.org"; option domain-name-servers 192.168.0.1;
option domain-search "mysite.org"; default-lease-time 14400; authoritative;


subnet 192.168.0.0 netmask255.255.255.0 { range 192.168.0.150 192.168.0.200;
        option routers 192.168.0.1; default-lease-time 14400; max-lease-time
        172800; host client {
                hardware ethernet.08:00:27:44:99:fc; fixed-address 192.168.0.2;
        }
}
```

Келтірілген мысалда MAC-мекенжайдың (hardware ethemet) көмегімен клиентті сәйкестендіру көрсетілген. Клиентке 192.168.0.2 IP-мекенжайы

мен *client* тораптың атауы тағайындалады. MAC-мекенжайды көптеген тәсілдермен анықтауға болады. Тіпті, оны сатып алған кезде берілген желілік тақша орамынан оқып алуға болады. Алайда, оны DHCP-сервердің жүйелік журналынан алу бәрінен де ыңғайлы болып табылады.

Осы конфигурацияны қолданып, журналған қарап көрейік:

```
2014-07-04T12:02:07.141285+04:00 server dhcpd: DHCPRE- LEASE of 192.168.0.150
from 08:00:27:44:99:fc (client) via enp0s8 (found)
2014-07-04T12:02:08.099148+04:00 server dhcpd: uid lease 192.168.0.150 for client
08:00:27:44:99:fc is duplicate on 192.168.0.0/24
2014-07-04T12:02:08.099661+04:00 server dhcpd: DHCPDISCOVER from
08:00:27:44:99:fc via enp0s8 2014-07-04T12:02:08.100182+04:00 server dhcpd:
DHCPOFFER on 192.168.0.2 to 08:00:27:44:99:fc via enp0s8
2014-07-04T12:02:08.101437+04:00 server dhcpd: uid lease 192.168.0.150 for client
08:00:27:44:99:fc is duplicate on 192.168.0.0/24
2014-07-04T12:02:08.101912+04:00 server dhcpd: DHCPREQUEST for
192.168.0.2 (192.168.0.1) from 08:00:27:44:99:fc via enp0s8
2014-07-04T12:02:08.102376+04:00 server dhcpd: DHCPACK on 192.168.0.2 to
08:00:27:44:99:fc via enp0s8
```

Алдындағы мысалға сәйкес қайталанатын өтпелі процесс жақсы көрінеді. Бұндай жағдайда «uid lease 192.168.0.150 for client 08:00:27:44:99:fc is duplicate on 192.168.0.0/24» сөйлемшесі клиент (MAC-мекенжай бойынша сәйкестендірілетін) екі рет: бірінші рет жалдаудың деректер қорында, ал екінші рет мекенжайды қолмен тағайындайтын конфигурация файлында кездесетінін көрсетеді.

Жалдау деректер қорының ішіндегісіне қарап көрейік:

```
server:/ # cat /var/lib/dhcp/db/dhcpd.leases
#   The format of this file is documented in the dhcpd. leases(5) manual page.
#   This lease file was written by isc-dhcp-4.2.5-P1

lease 192.168.0.150 {
        starts 5 2014/07/04 07:53:11;
        ends 5 2014/07/04 11:53:11;
        tstp 5 2014/07/04 11:53:11;
        cltt 5 2014/07/04 07:53:11;
        binding state active;
        next binding state free;
        rewind binding state free;
        hardware ethernet 08:00:27:44:99:fc;
        uid "\001\010\000'D\231\374";
        client-hostname "client";
}
server-duid "\000\001\000\001\033I\023\250\010\000'\313\ 371\237";
```

```
lease 192.168.0.150 {
        starts 5 2014/07/04 07:53:11; ends 5 2014/07/04
        08:02:07; tstp 5 2014/07/04 08:02:07; cltt 5 2014/07/04
        07:53:11; binding state free;
        hardware ethernet 08:00:27:44:99:fc;
```

Көріп тұрғанымыздай, Бұл MAC-мекенжай жалдау деректер қорында екі рет кездеседі және автоматты түрде жойылмайды – IP-мекенжайды жаңартуға қайтадан сұрау салған кезде сервердің жүйелік журналында да осындай хабарламаларды аламыз:

```
2014-07-04T12:07:39.690609+04:00 server dhcpd: DHCPRE- LEASE of 192.168.0.2
from 08:00:27:44:99:fc via enp0s8 (not found)
2014-07-04T12:07:40.426971+04:00 server dhcpd: uid lease 192.168.0.150 for client
08:00:27:44:99:fc is duplicate on 192.168.0.0/24
2014-07-04T12:07:40.428476+04:00 server dhcpd: DHCPDISCOVER from
08:00:27:44:99:fc via enp0s8 2014-07-04T12:07:40.430072+04:00 server dhcpd:
DHCPOFFER on 192.168.0.2 to 08:00:27:44:99:fc via enp0s8
2014-07-04T12:07:40.431012+04:00 server dhcpd: uid lease 192.168.0.150 for client
08:00:27:44:99:fc is duplicate on 192.168.0.0/24
2014-07-04T12:07:40.431563+04:00 server dhcpd: DHCPREQUEST for
192.168.0.2 (192.168.0.1) from 08:00:27:44:99:fc via enp0s8
2014-07-04T12:07:40.432093+04:00 server dhcpd: DHCPACK on 192.168.0.2 to
08:00:27:44:99:fc via enp0s8
```

dhcpd. leases артық жазбаларды мәтіндік редакторды қолдана отырып, қолмен өшіру қажет. Осы жазбаларды өшіріп, DHCP-серверді қайтадан іске қосып, клиенттен мекенжайды қайтадан сұраймыз:

```
2014-07-04T12:13:48.503103+04:00 server dhcpd: Internet Systems Consortium DHCP
Server 4.2.5-P1 2014-07-04T12:13:48.503129+04:00 server dhcpd: Copyright 2004-2013
Internet Systems Consortium. 2014-07-04T12:13:48.503129+04:00 server dhcpd: All
rights reserved.
2014-07-04T12:13:48.503129+04:00 server dhcpd: For info, please visit https://www.
isc.org/software/dhcp/ 2014-07-04T12:13:48.503129+04:00 server dhcpd:
WARNING: Host declarations are global. They are not limited to the scope you declared
them in. 2014-07-04T12:13:48.503189+04:00 server dhcpd: Not searching LDAP since
ldap-server, ldap-port and ldap- base-dn were not specified in the config file 2014-07-
04T12:13:48.503559+04:00 server dhcpd: Wrote 0 deleted host decls to leases file.
2014-07-04T12:13:48.513113+04:00 server dhcpd: Wrote 0 new dynamic host decls to
leases file.
2014-07-04T12:13:48.513126+04:00 server dhcpd: Wrote 0 leases to leases file.
2014-07-04T12:13:48.543124+04:00 server dhcpd: Listening on
LPF/enp0s8/08:00:27:cb:f9:9f/192.168.0.0 /24
```

2014-07-04T12:13:48.543125+04:00 server dhcpd: Sending on LPF/enp0s8/08:00:27:cb:f9:9f/192.168.0.0/24 2014-07-04T12:13:48.543126+04:00 server dhcpd[6870]: Starting ISC DHCPv4 4. x Server [chroot]..done 2014-07-04T12:13:48.543455+04:00 server systemd[1]: Started LSB: ISC DHCP 4.x Server.
2014-07-04T12:14:24.313498+04:00 server dhcpd: DHCPRELEASE of 192.168.0.2 from 08:00:27:44:99:fc via enp0s8 (not found)
2014-07-04T12:14:25.443591+04:00 server dhcpd: DHCPDISCOVER from 08:00:27:44:99:fc via enp0s8 2014-07-04T12:14:25.443591+04:00 server dhcpd: DHCPOFFER on 192.168.0.2 to 08:00:27:44:99:fc via enp0s8
2014-07-04T12:14:25.453519+04:00 server dhcpd: DHCPREQUEST for 192.168.0.2 (192.168.0.1) from 08:00:27:44:99:fc via enp0s8
2014-07-04T12:14:25.453519+04:00 server dhcpd: DHCPACK on 192.168.0.2 to 08:00:27:44:99:fc via enp0s8

Көріп тұрғанымыздай, жалдаудың қайталанатын жазбалары туралы ескертулері жоқ. Сервер қалыпты жұмыс істейді.

DHCP-опцияларды баптау. DHCP-да хаттамаға сәйкес сандық мәнмен сәйкестендірілетін көптеген әр түрлі опциялар сипатталған. Көптеген опциялар көпшілік мақұлдаған болып табылады және тікелей стандарттарда, мысалы, *domain-name-де* көрсетілген. Басқа жағынан көптеген опциялар осы стандарттарда сипатталмағанына қарамастан кеңінен қолданылады.

Proxy Auto Configure (PAC, или WPAD, — Web Proxy Auto Discovery) прокси-серверді автоанықтау - ең көп таралған қосымша опциялардың бірі болып табылады. Соның мысалы ретінде DHCP қосымша опциялар тапсырмасын қарап көрейік.

PAC жүйесі құрамында браузерге арналған прокси-серверді баптау сценарийі бар PAC файлдан және осы файлға іздеу салатын жүйеден тұрады. Файл толтырылып, прокси-серверсіз тікелей қол жетімді жергілікті желідегі кейбір Web-серверге жалпы қол жетімділігін береді.

/etc/dhcpd. conf –қа келесі жолдар қосылады:

```
# do windows-style proxy autoconfig: option local-proxy-config
code 252 = text;

subnet 192.168.0.0 netmask 255.255.255.0 {

    option local-proxy-config "http://www.example.org/ proxy.pac";
```

Екінші жол (түсініктемеден кейін) 252 кодымен DHCP опцияларының мәнін береді. Бұндай жағдай DHCP стандарттарында опция сипатталмағанына және оған ішкі және алдын ала белгілі болып табылатына байланысты болады. Бұндай сипаттамадан кейін *option* өрнегінің көмегімен басқалар сияқты осы опцияны да пайдалану мүмкін болады. Келтірілген мысалда PAC-файл http://www. *example. org/proxy. pac* мекенжайынан жүктелу керектігі көрсетілген.

3.2. DNS ҚЫЗМЕТІН БАПТАУ

DNS қызметі үш құрамдас бөліктен тұрады:

1. Иерархиялық құрылымда тұрғызылған *домен атауы* (domain name space) *мен ресурстік жазбалар* (resource records) *кеңістігі.* DNS иерархиялық ағашындағы *әр торап немесе парақ (аяқталған торап) қандай да бір ақпарат жиынтығын береді.* Осы ақпаратты алуға мүмкіндік беретін арнайы сұраулар бар. Сұраулар алуға қажетті жазбалардың атауы мен типтеріне нұсқайды. Мысалы, желілік тораптарды сәйкестендіру үшін A типті ресурстік жазбалар жиі қолданылады.
2. *DNS серверлері (атаулар сервері)* — домен ағашының құрылымы мен оның ішінде сақталатын ақпаратты сақтайтын серверлік бағдарламалық жасақ. Атаулар сервері домен ағашының құрылымын кэштей аладыдомен, алайда жалпы алғанда, атаулар сервері домен ағашының керекті үзіндісі сақталған басқа да атаулар серверіне нұсқауы мүмкін. Атаулар сервері өзі басқаратын домен құрылымына қатысты ғана толық ақпарат алады. Бұны домен зонасына авторитарлық иелік ету деп атайды. Авторитарлық ақпарат зоналар деп аталатын ұяшықтарда ұйымдастырылған және бұл зоналар жүйенің бұзылуға тұрақтылығын арттыратын атаулардың басқа серверлеріне автоматты түрде таралуы мүмкін.
3. *Атауларға рұқсат беру кітапханасы (resolver)* — Серверден ақпаратты клиенттерге ұсыну үшін алып шығуға қабілетті кітапхана

немесе бағдарламалар. Атауларға рұқсат беру кітапханасы сұрау салу үшін атаулардың ең болмағанда бір серверіне кіруге рұқсаты болуы тиіс. Әдетте, бұл кітапханалар ОС қоса салынған. Бұл атауларға рұқсат беретін API-кітапханасы арқылы жұмыс істейтін бағдарламашыға DNS хаттамасын білу қажеттілігінен құтылып кетуге мүмкіндік береді.

Осы DNS екі құрамдас бөлігі домендік жүйені ұсынудың үш деңгейіне өрескел сәйкес келеді.

1. Пайдаланушы тұрғысынан домендік жүйедегі ақпаратқа қол жеткізу кейбір жүйелік шақырулар арқылы (атаулар рұқсатының кітапханасы арқылы) жүзеге асырылады. Домендік жүйе пайдаланушыға бірдей шақырулармен кез келген қолда бар ақпаратты алуға болатын тұтас иерархиялық құрылым болып көрінеді.
2. Атаударға рұқсат беру тұрғысынан домендік жүйе атаулардың саны белгісіз серверлерден тұрады. Олардың әрқайсысы домендік ағаштың бір немесе бірнеше үзінділеріне ие. Атауларға рұқсат беру кітапханасы осы атаулар серверлерінен ақпаратты деректер қорынан алынған статистикалық ақпарат ретінде сұратады.
3. Атаулар сервері тұрғысынан домендік жүйе зона деп аталатын көптеген үзінділерден тұрады. Атаулар сервері кейбір зоналардың өзіндік көшірмелерін иеленуі мүмкін. Атаулар сервері зоналардың негізгі серверлерінен осы зоналардың жаңартылуын ұдайы сұрап тұруы қажет. Атаулар сервері клиенттерден түскен атауларға рұқсат беруге қатысты сұрауларын көп ағынды тәртіпте қарауы тиіс.

Негізгі ұғымдар. Домендік атаулар кеңістігінің ағаш тәрізді құрылымы бар. Ағаштың әр торабы мен парағына *ресурстік атаулар* сәйкес келеді. Домендік жүйе ақырғы торап пен ішкі торапты айыра алмайды, сол себепті өз ішінде «торап» деген бір термин пайдаланылады.

Әр тораптың ұзындығы 0-ден 63 таңбаға дейінгі белгісі бар. Көршілес тораптардың бірдей белгісі болуы мүмкін емес. Қатар тұрмайтын тораптардың ғана (әр түрлі ағашта орналасқан) қатар бірдей белгісі болуы мүмкін. Бір белгі резервтелген болып саналады – бұл бос белгі. Ол сұралған ағаштың түбірі ретінде пайдаланылады.

Тораптың домендік атауы — бұл домендік ағаштың торабынан бастап түбіне дейінгі барлық белгілердің реттілігі. Домендік атауды құратын белгілер солдан оңға, яғни, тым ерекшелерден азырағына қарай (түбіріне жақын) жазылады және оқылады.

Келісу бойынша домендік атаулар еркін тізілімде сақталуы мүмкін, алайда домендік атауларды салыстыру тізілімге тәуелсіз жүргізіледі. Мысалы, «а» торабы мен «А» торабын құруға болады, бірақ бұл тораптарды бір зонада құру мүмкін емес. Себебі бірегей сиректілігіне тексеру жасаған кезде тізілімге тәуелсіз салыстыру пайдаланылады.

Пайдаланушы домендік атауды жазған кезде барлық белгілер нүктемен бөлініп («.») жазылады. Себебі толық домендік атау түпкілікті тораптың

белгісімен (бос жолмен белгіленетін) аяқталуы тиіс. Бұл көзбен шолғанда толық домендік атау әрқашан нүктемен аяқталатынына әкеп соғады. Бұл жағдай екі мақсаты көздейді:

1) Толық домендік атауды (әдетте, абсолюттік деп аталатын) білдіретін таңбалы жолдарды пайдалану. Мысалы, «www.example.com.»;
2) Жоғарғы домендік тораптардың бастапқы белгілерін ғана білдіретін таңбалы жолдарды белгілеу. Бұл жол доменнің жергілікті атауымен толықтырылу керектігі тұспалданған. Бұндай белгілеу салыстырмалы домендік атау деп аталады. Мысалы, егер компьютердің жергілікті домендік атауы example. com болса, «www» домендік атауы салыстырмалы болады.

Әдетте салыстырмалы атаулар жұрнақтарды іздеу тізімінің жергілікті жүйесінде бапталған домендік атауларын көрсету үшін пайдаланылады. Олар көбінесе, пайдаланушы интерфейстерде кездеседі де, DNS жергілікті жүйесінің бапталуына байланысты олардың пайымдаулары өзгертілуі мүмкін. Жалпы, салыстырмалы атаулар домендік атауларды іздеу тізімінде «.» түпкілікті зонасын айқын емес қосады. Осылайша, «www.example.com.» домендік атауды сәйкестендіру үшін «www. example. com» атауын пайдалануға болады.

Домен өз домендік атауымен анықталады және осы доменде немесе одан төмен тұрған домендік кеңістіктен тұрады. Домен басқа доменнің қосалқы домені болып табылады, егер де ол осы доменге енгізілсе. Мысалы, «A. B.C.D» домені «B. C. D», «C. D», «D» және «.» домендері үшін қосалқы домен болып табылады.

Ресурстік жазбалар. Домендік атау торапты теңдестіреді. Әр тораптың ақпараттар жиынтығы бар. Олар бос және жалпы алғанда ресурстік жазбалар жиынтығынан (Resource Record — RR) тұруы мүмкін. Тораптағы ресурстік жазбалар тәртібінің мәні жоқ. Сол себепті DNS-сервер жұмыс процесінде еркін өзгерте алады.

Ресурстік жазба мына өрістерден тұрады:

1) *Owner*(иеленуші) — осы ресурстік жазба қай торапқа жататынын анықтайды;
2) *Type*(тип) — жазбаның типін анықтайды. Тип 16-бит мәнімен анықталады. Типтердің кейбір мәндері кейінге сақталған. Соның ішінде негізгілері:
   - A — желілік торап мекенжайын анықтайтын мекенжай жазбасы;
   - *CNAME* — желілік торап лақабының канондық атауын анықтайды;
   - *MX*— осы торап үшін пошта алуға пайдаланатын серверлерді анықтайды;
   - *NS* — осы торап үшін авторитарлық серверлерді анықтайды;
   - *PTR* — кері зоналарды құрғанға дейін пайдаланылатын домендік атаулар кеңістігіне сілтеуіш;
   - *SOA*(start of authority) — авторитарлық зонаның басын анықтайды;
3) *Class*(класс) — осы жазба ұсынылатын хаттамалар ортасы. Бұнда IN (the

Internet system) және CH (the Chaos system) көрсетілуі мүмкін. Қазіргі уақытта іс жүзінде барлық серверлер IN жазбасын ғана пайдаланады;

4) *TTL*(time to live) — жазба болмысының уақыты. Бұл параметр осы жазбаны басқа да DNS-серверлерге қанша уақытта кэштеуге рұқсат етілген кезеңді анықтайды;

5) *RDATA*— ресурстік жазбалардың тікелей құрамы. Құрамындағының пішімі таңдалған жазба типіне байланысты болады.

Зоналарды құру. ICS Bind 9 — өз зоналары жоқ кэштелген DNS-серверді мысал ретінде алып, қарапайым жағдайды қарастырып көрейік. Bind конфигурациясы мынадай:

```
server:/etc # cat named.conf options {
        directory "/var/lib/named"; listen-on port 53 { any; };
};

zone "." in {
        type hint;
        file "root.hint";
};
```

Bind серверін қайта іске қосып, сұрауға жауап береді ме екенін қараймыз:

```
server:/etc # renamed restart redirecting to systemctl restart
named server:/etc# host www. mail. rulocalhost Using domain
server:
Name: localhost Address: 127.0.0.1#53 Aliases:

www. mail. ru has address 94.100.180.70 www. mail. ru has
address 217.69.139.70
```

Конфигурациялық параметрлерді толығырақ қарап көрейік. *Directory* опциясы барлық Bind файлдар, ол жұмыс істеген кезде, қай жерде сақталатынын көрсетеді. *listen-on* опциясы Bind-тің клиенттерден сұрау салу үшін тыңдалып отыратын IP-мекенжайы мен портына нұсқайды. Бұл сервердің жалпы опциялары.

Кэштелген DNS-серверлерді құрудың екі амалы бар: бас серверлерді пайдалану және түпкілікті зонаны пайдалану. Бірінші амал - осы серверге белгісіз барлық сұрауларды басқа DNS-сервер - DNS Forwarder-ге жіберу болып табылады. Осылайша сұрауларды ұйымдастыру DNS-серверлерді сол бас DNS-серверлерге тәуелді етеді. Олардан бас тартқан кезде бапталатын DNS-сервер бөгде домен атауларына рұқсат бере алмайды (соның ішінде, келтірілген mail. ru мысалы).

Екінші амал DNS-серверде *hint* (жасырын айту) сияқты арнайы зонаны құруды білдіреді. Бұл зонаның құрамында тек түпкілікті DNS-сервердің IP-мекенжайлары туралы ақпарат болады. Демек, бөгде домендерге рұқсат

беру бас серверлерге тәуелді емес және бапталып жатқан DNS-сервер түбірінен бастап домендік жүйеге дейін тікелей жүгінеді. *hint* зонасында бұзылуға тұрақтылықты едәуір арттыратын 10-нан астам түпкілікті DNS-сервер бар.

Осылайша, серверге салынған барлық сұраулар атаулардың түпкілікті серверлеріне қайта бағытталған.

Өте ыңғайлы ретке келтіру үшін конфигурацияға сұрауларды журналдау баптауын қосамыз:

```
options {
        directory "/var/lib/named"; listen-on port
        53 { any; };
};
logging {
        channel query logging {
                file "/var/log/named querylog" versions 3 size
                100M; print-time yes;
        };
        category queries { query logging;
        };
};

zone "." in {
        type hint;
        file "root.hint";
};
```

Бұл жерде үш соңғы нұсқаның әрқайсысы 100 Мбайттан аспай сақталатын */var/log/name_querylog* файлында жолданған query_logging журналдау арнасы құрылған. *queries* хабарламалар санаты *query_logging* арнасына журналдауға бағытталған.

Атауға рұқсатты тағы бір мәрте сұрап алып, жаңа журналдың мәнін қарап көрейік:

```
server:/var/lib/named/log # host www. mail. ru localhost Using domain server:
Name: localhost Address: 127.0.0.1#53 Aliases:

www. mail. ru has address 217.69.139.70 www. mail. ru has address 94.100.180.70
server:/var/lib/named/log # cat named querylog 04-Jul-2014 12:45:56.034 client
127.0.0.1#38904 (www. mail.ru): query: www.mail.ru IN A + (127.0.0.1) 04-Jul-2014
12:45:57.334 client 127.0.0.1#43435 (www. mail.ru): query: www.mail.ru IN AAAA +
(127.0.0.1) 04-Jul-2014 12:45:58.343 client 127.0.0.1#42373 (www. mail.ru): query:
www. mail. ru IN MX + (127.0.0.1)
```

Жергілікті домен зоналарын құру. Жергілікті домен зонасын құрып көрейік. Ол үшін */etc/named. conf* файлында оның конфигурациясын

қосамыз:

```
options {
        directory "/var/lib/named"; };
logging {
        channel query logging {
                file "/var/log/named querylog" versions 3 size
                100M; print-time yes;
        };
        category queries { query logging;
        };
};

zone "." in {
        type hint;
        file "root.hint";
};
                                        zone "mysite.org" in {
                                            type master;
        file "master/mysite.org";
};
```

Жаңадан қосылған зона *master* типіне ие, яғни бұл ағымдағы серверде сақталып редакцияланатын негізгі зона. *file* нұсқауы зонаның деректері бар файлдың орналасқан жерін сипаттайды (файл DNS-сервердің негізгі баптауларының *directory* нұсқауына қатысты көрсетілген). Осы файлға сайттың минималды конфигурациясын жазып көрсетейік:

```
    server:/etc # cat /var/lib/named/master/mysite. org $TTL 1W
@                                   IN SOA
org. root.server.mysite.org. (

serial (d. adams) refresh

retry

                        IN NS           server
server                  IN A            192.168.0. 1
client                  IN A            192.168.0. 2

expiry

minimum
```

Толығырақ қарап көрейік. Бұл файл *mysite.org* (*named.conf* файлын қарау) зонасының жұмысын қамтамасыз ету үшін бапталған. Зона файлындағы зона атауы «@» таңбасымен ауыстырылуы мүмкін. Бірінші жол кэштелген серверлердегі

жазбалар болмысын тағайындайды. Екінші жол бұдан бұрын айтып кеткен SOA жазбасын сипаттайды. Оның қырларын қарастырып көрейік:

- *server.mysite. org.*— зона атауы;
- *root.server.mysite.org.*— осы домен әкімшісінің пошталық мекенжайы (бірінші нүктені «@»-қа ауыстыру арқылы);
- *1*— сериялық нөмір;
- *2D*— зонаны бағыңқы серверлермен жаңарту уақыты;
- *4H*— жаңарту сәтсіз өткен жағдайда зонаны жаңартуға қайтадан әрекеттену уақыты;
- *6W*— зонаның жарамдылық мерзімі аяқталған уақыт;
- *1W*— үнсіз келісім бойынша жазбалар болмысының ең кем уақыты.

Зонаны жаңарту — бұл зонаны негізгі серверден бағыңқы немесе еншілес серверге (slave) синхрондау процесі. Оның нәтижесінде бағыңқы сервер зонаның толық көшірмесіне ие болады. Бұзылуға тұрақтылығын арттыру үшін қолданылады.

Сериялық нөмір де зонаны синхрондау кезінде пайдаланылады. Бағыңқы сервер зона туралы барлық ақпаратты әрқашан өзіне көшірмелеудің орнына, тек SOA жазбасына сұрау салып, зонаның сериялық нөмірі өзгерген-өзгермегенін тексереді. Егер зонаның сериялық нөмірі бағыңқы серверлерден гөрі негізгі серверлерде көбірек болған жағдайда бағыңқы сервер зонаның жаңартылуын сұрайды:

```
IN NS          server
```

Бұл жазба ағымдағы зонаға (зонаның атауы көрсетілмеген — зона үнсіз келісім бойынша пайдаланылады)атаулар серверін қосады. Атаулар сервері осы зонаға қызмет көрсететін атаулардың қолданыстағы серверлерін таратпау үшін күрделі конфигурацияларда және зонаны жаңарту кезінде (бағыңқы серверлер өз зоналарын кезекті жоспарлы синхрондауды тоспай, әпсәтте жаңартуы үшін) жарияланымды жіберу үшін сервердің өзімен пайдаланылады. Сондағы бұндай жазбалар еншілес зоналар (бағыңқы домендер) баптауының бас зоналарының құрамында болады:

```
server          IN A          192.168.0.1
client          IN A192.168.0.2Бұл - мекенжай жазбалары, яғни IT-
мекенжайлар DNS-атаулармен тікелей салыстырылатын жазбалар.
DNS-атаулар соңында нүктесіз көрсетілген. Ал бұл оларға зона
атауларын қосу қажеттілігін білдіреді, яғни бұл жазбалар
мыналарға толық ұқсас:
server.mysite.org.          IN A          192.168.0.1
client.mysite.org.          IN A          192.168.0.2
```

DNS-серверді қайтадан іске қосып, жүйелік журналға не түсетінін қарап көрейік:

Rcnamed restart

tail /var/log/messages

2014-07-04T20:08:44.011458+04:00 server named[9562]: zone mysite.org/IN: loaded serial 1

2014-07-04T20:08:44.011458+04:00 server named[9562]: all zones loaded

2014-07-04T20:08:44.011459+04:00 server named[9562]: running

2014-07-04T20:08:44.011459+04:00 server named[9517]: Starting name server BIND ..done

Зона сәтті жүктелгендіктен, оны *dig* командасының көмегімен тексереміз*:*

server:/var/lib/named/master # dig server. mysite.org @127.0.0.1

; <<>> DiG 9.9.4-rpz2.13269.14-P2 <<>> server.mysite. org @127.0.0.1 ;; global options: +cmd ;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:

14946

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096 ;; QUESTION SECTION:

;server. mysite. org. IN A

;; ANSWER SECTION:

server.mysite.org. 604800 IN A 192.168.0.1 ;; AUTHORITY SECTION:
mysite.org. 604800 IN NS server.mysite.org.
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Jul 04 20:14:57 MSK 2 014 ;; MSG SIZE rcvd: 76

Bind DNS-серверімен бірге жинақтамада жеткізілетін *dig* командасы - ретке келтірудің ең ыңғайлы құралы болып табылады. Оны іске қосқан кезде рұқсат алуға әрекет жасап көру қажеттілігі туындайтын мекенжай және тиісті сұрауды жолдау қажеттілігі туындайтын сервердің мекенжайы («@» таңбасынан кейін) көрсетіледі. Қай серверден *dig* командасы жауап алғаны көрсетілген *SERVER:* (астыңғы жағынан 3-ші) жолына назарыңызды салыңыз.

Сондай-ақ серверге басқа да сұраулар жолдауға болады:

server:/var/lib/named/master # dig -t soa mysite.org @127.0.0.1

; <<>> DiG 9.9.4-rpz2.13269.14-P2 <<>> -t soa mysite. org @127.0.0.1
;; global options: +cmd ;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3246 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096 ;; QUESTION SECTION:
;mysite.org. IN SOA

;; ANSWER SECTION:
mysite.org. 604800 IN SOA server.mysite.org.
root. server. mysite.org. 1 172800 14400 3628800 604800

;; AUTHORITY SECTION:
mysite.org. 604800 IN NS server.mysite.org.

;; ADDITIONAL SECTION:
server.mysite.org. 604800 IN A 192.168.0.1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Jul 04 20:16:26 MSK 2 014 ;; MSG SIZE rcvd: 117

DNS Server қызметінің клиентін баптау. DNS қызметінің клиенті — бұл атауларға рұқсат беретін жүйелік кітапхана (resolver). Posix- жүйелерде ол */etc/resolv. conf* файлында бапталады.

Баптау файлының келесі түрі бар:

server:/etc # cat /etc/resolv.conf search mysite. org
nameserver 192.168.0.1

Ол екі негізгі нұсқаудан тұрады: *search* және *nameserver*. *search* нұсқауы домен журнақтарының тізімін, ал *nameserver* — жүйемен пайдаланылатын атаулар серверін анықтайды. Мысалы, егер атаулар серверін көрсетпей *dig* командасын іске қоссақ, ол сервердің IP-мекенжайын мына файлдан алады:

server:/etc # dig client.mysite.org

; <<>> DiG 9.9.4-rpz2.132 69.14-P2 <<>> client. mysite. org
;; global options: +cmd ;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9676 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096 ;; QUESTION SECTION:
;client. mysite. org. IN A

;; ANSWER SECTION:

client.mysite.org. 604800 IN A 192.168.0.2 ;; AUTHORITY SECTION:
mysite.org. 604800 IN NS server.mysite.org.

;; ADDITIONAL SECTION:

server.mysite.org. 604800 IN A 192.168.0.1 ;; Query time: 0 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Fri Jul 04 20:19:24 MSK 2 014 ;; MSG SIZE rcvd: 99

Осы параметрді көрсеткеннен кейін барлық ОС қызметтері желілік атауларға рұқсат бере алады:

server:/etc # ping -c 2 client. mysite. org
PING client. mysite.org (192.168.0.2) 56(84) bytes of
data.
64 bytes from 192.168.0.2: icmp seq=1 ttl=64 time=0.000 ms 64 bytes from 192.168.0.2:
icmp seq=2 ttl=64 time=0.000 ms

---- client.mysite.org ping statistics ----------
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.000/0.000/0.000/0.000 ms

Домен атауларының жұрнақтар тізімі тораптың толық емес атауы бойынша IP-мекенжайды іздеу үшін пайдаланылады. Келтірілген мысалда бір *mysite. org* доменінен тұратын жұрнақтар тізімі көрсетілген. DNS клиенті IP-мекенжайға рұқсат беру сұрауын алған кезде толық мекенжай ретінде рұқсат беру әрекеті сәтсіз өткеннен кейін домен атауының соңында домен атауларының әр жұрнақтарын кезекпен «жазып бітіруге» әрекет жасап көруі тиіс:

server:/etc # ping client
PING client. mysite.org (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp seq=1 ttl=64 time=9.95 ms ЛС
---- client.mysite.org ping statistics ----------
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 9.954/9.954/9.954/0.000 ms server:/etc # tail
/var/lib/named/log/named querylog

04-Jul-2014 20:30:58.702 client 192.168.0.1#52382 (client.mysite.org): query:
client.mysite.org IN A + (192.168.0.1)
04-Jul-2014 20:30:58.712 client 192.168.0.1#58472 (2.0.168.192.in-addr.arpa): query:
2.0.168.192.in- addr.arpa IN PTR+ (192.168.0.1)

Осылайша, домен атауларының жұрнақтар тізімі толық емес домен

атаулары рұқсат етілетін тәртіпті анықтайды. Мысал ретінде табиғатта жоқ домен атауының рұқсатын қарап көрейік:

```
server:/etc # ping -cl idontexist ping: unknown host idontexist
server:/etc # tail /var/lib/named/log/named querylog

04-Jul-2014 20:33:19.842 client 192.168.0.1#55836 (idontexist.mysite.org): query: idontexist.mysite.org IN A + (192.168.0.1)
04-Jul-2014 20:33:19.842 client 192.168.0.1#40342 (idontexist): query: idontexist IN A + (192.168.0.1)
```

Домен жұрнақтары бойынша табу мүмкін болмаған кезде DNS клиенті көрсетілген мекенжайды толық домен атауы деп есептеп, DNS-да жазбаны табуға тырысып талпынатыны көрініп тұр.

DNS қызметін пайдалана отырып, түйіндер атауларына рұқсат беру процесін баптау. Автоматты түрде DHCP көмегімен DNS баптауы қалай іске асырылатынын қарап көрейік. Бұдан бұрын DHCP конфигурациясын құрылуы сипатталған болатын. Ал енді DNS тізбегіндегі осы конфигурацияның баптауын қарап көрейік.

Тестілік тәртіпте *dhcpcd* бағдарламасын пайдаланып көрейік:

```
client:~ # dhcpcd enp0s3 -T IPADDR='192.168.0.2'
NETMASK='255.255.255.0'
NETWORK='192.168.0.0'
BROADCAST='192.168.0.255'
ROUTES=''
GATEWAYS='192.168.0.1'
DNSDOMAIN='mysite.org'
DNSSEARCH='mysite.org'
DNSSERVERS='192.168.0.1'
DHCPSID='192.168.0.1'
LEASETIME='14400'
RENEWALTIME='0'
REBINDTIME='0'
INTERFACE='enp0s3'
CLASSID='dhcpcd 3.2.3'
CLIENTID='01:08:00:27:44:99:fc'
DHCPCHADDR='08:00:27:44:99:fc'
```

Қорытынды DNS-тың дұрыс баптаулары келтірілгенін көрсетеді. Клиент DHCP қайта іске қосқаннан кейін ол жергілікті атауларға рұқсатты автоматты түрде реттейді:

```
client:~ # cat /etc/resolv.conf # Generated by dhcpcd for interface enp0s3 search mysite.org nameserver 192.168.0.1
```

Атауларға қол жеткізуге рұқсат беруді баптауға DHCP-серверінен домен

атауларының жұрнақтарынан басқа, атаулар серверінің өзі де түседі. Ары қарай осы тораптағы атауларға қол жеткізуге рұқсат беру сәтті өтеді: client:~ # dig www. mail. ru

; <<>> DiG 9.9.3-rpz2+rl.156.01-P2 <<>> www. mail. ru ;; global options: +cmd ;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35354 ;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 5
;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 4096 ;; QUESTION SECTION:
IN A
;www. mail. ru.
;; ANSWER SECTION:
www. mail. ru. 60 IN A 217.69. 139.70
www. mail. ru. 60 IN A 94.100. 180.70
;; AUTHORITY SECTION:
mail. ru. 600 IN NS ns1.mail. ru.
mail. ru. 600 IN NS ns2. mail. ru.
;; ADDITIONAL SECTION:
ns1. mail. ru. 343666 IN A 217. 69.139.112
ns1. mail. ru. 600 IN AAAA 2a00 :1148:db00
ns2. mail. ru. 343666 IN A 94.100.180.138
ns2. mail. ru. 600 IN AAAA 2a00 :1148:db00
;; Query time: 160 msec ;; SERVER: 192.168.0.1#53(192.168.0.1) ;; WHEN: Fri Jul 04 20:43:00 MSK 2 014 ;; MSG SIZE rcvd: 196

Запрос из своего домена:

client:~ # dig server. mysite.org
; <<>> DiG 9.9.3-rpz2+rl.156.01-P2 <<>> server. mysite. org
;; global options: +cmd ;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22179
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096 ;; QUESTION SECTION:
;server.mysite.org. IN A
;; ANSWER SECTION:
server.mysite.org. 604800 IN A 192.168.0.1 ;; AUTHORITY SECTION:
mysite.org. 604800 IN NS server.mysite.org.
;; Query time: 0 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Fri Jul 04 20:43:17 MSK 2 014 ;; MSG SIZE rcvd: 76

Қысқа домен атауларынакешт шеттегі бағдарламалар арқылы пайдалану әрекеті де оңды нәтиже көрсетеді:

```
client:~ # ping -c1 server
PING server. mysite.org (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp seq=1 ttl=64 time=0.000 ms

---- server. mysite.org ping statistics ----------------------------------
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.000/0.000/0.000/0.000 ms
```

3.3. ДОМЕННІҢ АҚПАРАТТЫҚ ЖҮЙЕСІН БАПТАУ

Active Directory — бұл LDAP – үйлесімді (Lightweight Directory Access Protocol — каталогтарға қатынаудың жеңілдетілген хаттамасы) *Microsoft корпорациясының каталогтар қызметін іске асыру.*

Active Directory объектілерден тұратын сатылы құрылымы бар. *Объектілер* деп пайдаланушылар мен компьютерлердің ресурстары, қызметтері мен есептік жазбалары түсініледі. Active Directory объектілер туралы ақпарат ұсынады, объектілерді ұйымдастыруға, оларға қатынауды басқаруға мүмкіндік береді, сондай-ақ қауіпсіздік ережелерін анықтайды.

Доменнің бақылаушысы деп Active Directory-де домендік қызметтер орындалатын сервер аталады.

Active Directory құрылымына мыналар кіреді:

- Орман Active Directory — Active Directory-дегі барлық объектілердің, атрибуттар мен ережелердің жиынтығы. Орманда бір немесе бірнеше ағаш бар, олар сенімнің транзитивтік қатынастарымен байланысқан. Ағаш бір немесе бірнеше доменді қамтиды. Үнсіз келісім бойынша орманда бір домен болады, ол орманның тамырлы домені ретінде белгілі;
- DNS аттарымен – аттар кеңістіктерімен өзінің құрылымдарымен сәйкестендірілетін домендер;
- домендердің бөлімшелері — контейнерлер, оларда домендегі объектілер топталуы мүмкін.

Орман ұйымдастыру үшін қорғаныш шекара сияқты әрекет етеді және әкімшілер өкілеттіктерінің көлемін айқындайды.

Бөлімшелер доменнің ішіндегі сатыластықты құруды мүмкін етеді, оған әкімшілендіруді жеңілдетеді және Active Directory-де компанияның құрылымын модельдеуге мүмкіншілік береді. Бөлімшелердің басқа бөлімшелері болуы мүмкін

және әкімшілік өкілеттіктерді табыстауға болатын ең төмен деңгей болып табылады. Бөлімшелердің болуы құқықтарды табыстауды жеңілдетеді: иегерлер объектілерді басқару құқықтарын басқа пайдаланушыларға немесе топтарға бере алады.

Active Directory домендік қызметтері каталогтардың деректерін сақтайды және пайдаланушы мен домендер арасындағы өзара әрекетін басқарады.

Active Directory домендік қызметтері — бұл ОЖ Windows Server 2008 сервердің ролі. Бұл қызметтер бөлінген каталогтың қызметі болып табылады, оны орталықтандырылған және қауіпсіз желі үшін пайдалануға болады.

Әкімшілік доменінің құралдарын орнату және конфигурациялау. Windows Server 2008 жаңа орманын орнату үш тәсілмен мүмкін болады:

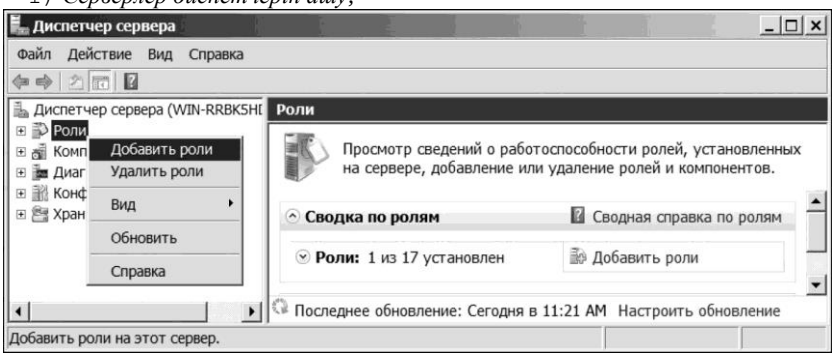
1) Windows интерфейсін пайдаланумен жаңа орман орнату;
2) Командалық жолды пайдаланумен жаңа орман орнату;
3) *Жауаптар файлын пайдаланумен жаңа орман орнату.*

Windows интерфейсін пайдаланумен жаңа орман орнату.

Windows интерфейсі Active Directory домендік қызметтерді орнатудың бірнеше нұсқаларынан тұрады. Әрі қарай Рөлдерді қосу шеберінің көмегімен домендік қызметтерді орнату қаралады, оған сервер диспетчерінде қол жеткізуге болады.

Рөлдерді қосу шеберінің көмегімен жаңа орманды орнату үшін мына іс-қимылдарды орындау:

1) *Серверлер диспетчерін ашу;*



3.1-сурет. Сервер диспетчеріне жаңа Рөлді қосу

2) *Рөлдер бойынша мәлімет* терезесінде *Рөлдер қосу* батырмасын басу немесе мәнмәтіндік мәзірдің көмегімен *Рөлдер* торабы бойынша *Рөлдер қосу* (3.1-сурет) командасын таңдау;
3) С*ервердің Рөлдерін таңдау* бетінде *Active Directory-дің домендік қызметтері* опциясын таңдап, *Әрі қарай* батырмасын басу;
4) *Таңдалған элементтерді растаңыз* бетіндегі *Орнату* батырмасын басу;

5) *Орнатудың нәтижелері* бетінде «*Осы шеберді жауып, Active Directory домендік қызметтерін орнатудың шеберін іске қосыңыз* (dcpromo.exe)» тармағын таңдау;
6) «*Сіз Active Directory домендік қызметтерін орнатудың шеберіне келдіңіз*» пайда болған терезеде *Әрі қарай* батырмасын басу. Егер шеберді орнатудың кеңейтілген режимінде іске қосу талап етілсе, онда *Әрі қарай* батырмасын басудың алдында *Орнатудың кеңейтілген режимін пайдалану* опциясын таңдау керек*;*
7) Шебердің жұмысының келесі қадамында Windows Server 2008 және Windows Server 2008 R2 доменінің бақылауыштары үшін қауіпсіздік параметрлері туралы ақпарат ұсынылады. Ескертуді оқып шыққаннан кейін, *Әрі қарай* батырмасын басу керек;
8) *Өрістету конфигурациясын таңдаңыз* бетінде *Жаңа орманда жаңа домен құруды* таңдап, *Әрі қарай* батырмасын басу;
9) Орманның тамырлы доменінің атын көрсету және *Әрі қарай* батырмасын басу (Windows Server 2008 R2 жүйесінде Dcpromo. Exe бағдарламасы доменнің бір компонентті DNS-атын құруды мүмкін етпейді); егер шебер орнатудың кеңейтілген режимінде қосылса, онда доменнің NetBIOS-атын енгізуге арналған бет ашылады;
10) әрі қарай орманда орнату жоспарланатын доменнің бақылауыштарына арналған орманның жұмыс режимін таңдап, *Әрі қарай* батырмасын басу*;*
11) әрі қарай доменде орнату жоспарланатын доменнің бақылауыштарына арналған орманның жұмыс режимін таңдап, *Әрі қарай* батырмасын басу;
12) егер шебер DNS-сервер үшін табыстауды құра алмаған жағдайда келесі бет DNS-серверді орнатуды таңдау мүмкіндігін береді, табыстауды қолмен тапсыруға болатыны туралы ескерту жазылған сұхбат терезесі пайда болады. Әрі қарай жалғастыру үшін *Иә* батырмасын басу керек;
13) деректер базасына, журналдың файлдарына және SYSVOL папкасына арналған жайғасымды көрсету керек (немесе мәндерді үнсіз келісім бойынша қалдыру);
14) *Каталогтар қызметтерін қалпына келтіру режиміне арналған әкімшінің паролі* бетінде қалпына келтіру паролін енгізу және растау керек, сонан соң *Әрі қарай* батырмасын басу қажет. Бұл пароль автономды режимде орындалатын міндеттерге арналған каталогтар қызметтерін қалпына келтіру режимінде домендік қызметтерді қосу кезінде қажет етіледі;
15) келесі қадамда жауаптар файлында таңдалған баптауларды сақтаудың мүмкіншілігі ұсынылады, оны домендік қызметтермен әрі қарай жұмысты автоматтандыру үшін пайдалануға болады. Баптауларды файлға сақтау үшін *Параметрлерді экспорттау* батырмасын басып, жауаптар файлының атын енгізу және *Сақтау* батырмасын басу керек*;*
16) соңғы кезеңде шебер домендік қызметтердің баптауларын орындайды. Аяқталған соң Пайдаланушыға серверді автоматты түрде қайта жүктеу опциясын таңдау керек болады.

Командалық жолды пайдаланумен жаңа орманды орнату. Автоматтық орнату параметрлерінің тізімі мен олардың мәндері бар болғанда, оларды тікелей командалық жолда енгізуге болады. Параметрлердің мәндерін жауаптар файлынан алуға болады.

Сондай-ақ жауаптар файлының өзін пайдалануға болады, сонан соң сол командалық жолда автоматтық орнату параметрлерінің тізімі мен олардың мәндерін енгізуге болады. Мұндай жағдайда командалық жолдың параметрлері жауаптар файлында аталған барлық параметрлерге қосымша орнатылады.

Командалық жол арқылы доменнің жаңа бақылауышын орнату үшін келесі жолды енгізу керек, сонан соң «Енгізу» пернесін басу қажет:

dcpromo /unattend /ReplicaOrNewDomain=Domain / NewDomain=Forest
/NewDomainDNSName=ad. example /
DomainNetbiosName=AD /InstallDNS=Yes /ConfirmGc=Yes /
CreateDNSDelegation=No /SafeModeAdminPassword="Қауіпсіз режимге арналған пароль" /RebootOnCompletion=No

Автоматтық орнатудың параметрлерінің сипаттамасы «*dcpromo/?» командасының көмегімен қол жетімді болады*.

Жауаптар файлын пайдаланумен жаңа орман орнату. Жаңа орман орнату мақсатында жауаптар файлын құру үшін мынадай-іс-қимылдарды орындау қажет*:*

1) Блокнотты немесе кез келген мәтіндік редакторды ашу;
2) файлға келесі мәтінді енгізу (әрбір жолға бір-бір жазбадан):

```
[DCInstall]
ReplicaOrNewDomain=Domain
NewDomain=Forest
NewDomainDNSName=ad.example
ForestLevel=2
DomainNetbiosName=AD
DomainLevel=2
InstallDNS=Yes
ConfirmGc=Yes
CreateDNSDelegation=No
DatabasePath="C:\Windows\NTDS"
LogPath="C:\Windows\NTDS"
SYSVOLPath="C:\Windows\SYSVOL"
SafeModeAdminPassword="қалпына келтіру режимінің паролі"
```

3) файлды сақтау.

Жауаптар файлын пайдаланумен доменнің жаңа бақылауышын орнату үшін командалық жолда келесі көрсетілген команданы енгізу және «Енгізу» пернесін басу керек:

dcpromo /unattend:"< файлға жол>".

Орманды жою. Құрылған орманды жою үшін бірнеше тәсіл бар. Олардың ең қарапайымы — орнату шеберін іске қосу / жаңа орманды жою. Шебер *Қосу/ Орындау мәзірі арқылы* мәзірінің тармағы арқылы қол жетімді, пайда болған терезеде *dcpromo* командасын енгізіп, «*Енгізу*» пернесін басу керек.

Қолданыстағы орманды командалық жолдың көмегімен жою үшін келесі командаларды пайдалану қажет:

dcpromo /unattend /RetainDcMetadata=No / IsLastDCInDomain=Yes /RemoveApplicationPartitions=Yes /AdministratorPassword="Әкімшінің паролі" / RebootOnCompletion=No

Active Directory әкімшілендіру орталығы. Windows Server 2008 операциялық жүйесі Active Directory әкімшілендіру орталығында каталогтар қызметінің объектілерін басқаруды мүмкін етеді.

Active Directory әкімшілендіру орталығы Windows PowerShell командалық жолдың интерфейсінің технологиясына негізделген және желі әкімшілеріне Active Directory деректерін басқару бойынша кеңейтілген мүмкіншіліктер береді.

Active Directory әкімшіліендіру орталығы әкімшілендірудің келесі міндеттерін орындауды мүмкін етеді:

- есептік жазбаларды құру және оларды басқару;
- топтар құру және оларды басқару;
- компьютерлердің есептік жазбаларын құру және оларды басқару;
- бөлімшелер немесе контейнерлер құру және оларды басқару;
- доменге немесе доменнің бақылауыштарына қосылу, каталогтың деректерін қарап шығу және оларды басқару;
- сұрату құралдарын іздеудің көмегімен Active Directory деректерін сүзгіден өткізу.

Каталогтарға қатынаудың жеңілдетілген хаттамасы. AD LDS — бұл каталогтардың қызметі, ол LDAP (Lightweight Directory Access Protocol —каталогтарға қатынаудың жеңілдетілген хаттамасы) хаттамасы бойынша жұмыс істейді және каталогтармен жұмысқа бағдарланған қосымшаларды икемді қолдауды қамтамасыз етеді. AD LDS қызметі AD DS функционалдық мүмкіншіліктердің көпшілігін қамтиды, алайда оның жұмысы үшін домендерді өрістету жүргізуді немесе домендердің бақылауыштарын пайдалану талап етілмейді. Бір компьютерде AD LDS бірнеше данасын бірден қосуға болады, бұл кезде әр дана өзінің меншікті, тәуелсіз басқарылатын схемасын пайдаланатын болады.

AD LDS ролін орнату. AD LDS ролін орнату үшін «Сервер диспетчері» жабдығында *Рөлдер* торабын таңдау қажет және осы торап үшін мәнмәтіндік мәзірдің *Рөлдер қосу* командасын таңдау қажет. Пайда болған сұхбат терезесінде *Каталогтарға жеңіл қатынаудың Active Directory қызметтері* опциясын таңдап, *Әрі қарай* батырмасын басу керек, шебердің соңғы терезесінде *Орнату* батырмасын басу. Сонан соң шебердің көмегімен AD LDS қызметінің даналарын құруға болады. Ол үшін *Бастау* мәзірінде *Әкімшілендіру/AD LDS қызметтерін*

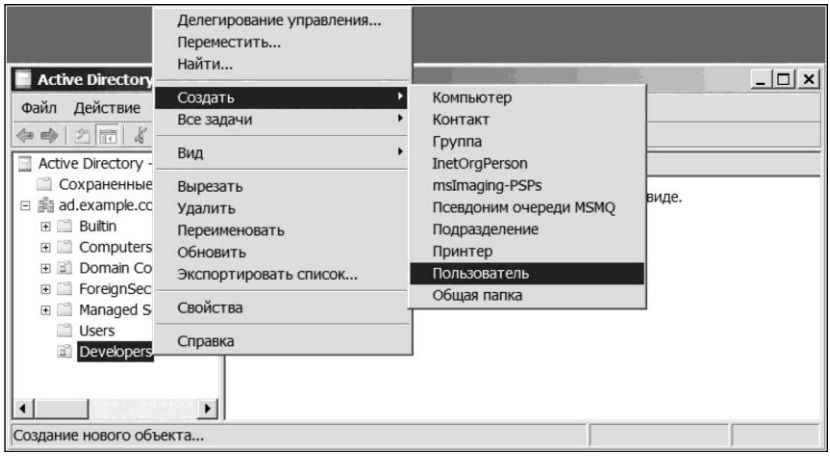
орнату шеберін таңдау қажет.

Пайдаланушының есептік жазбаларын құру. Пайдаланушының есептік жазбаларын құру әкімшілендіруде маңызды рөл атқарады. Есептік жазба түпнұсқалығын домен тексеретін дәл сол деректермен компьютерлерге және домендерге кіруге, сондай-ақ рұқсаттардың негізінде доменнің ресурстарына қатынауға мүмкіншілік береді.

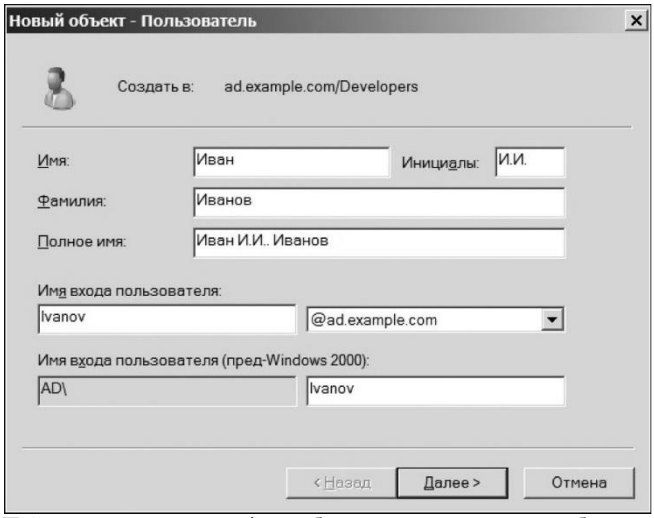
Әрі қарай пайдаланушылардың есептік жазбаларын құрудың түрлі нұсқалары қаралатын болады.

«Active Directory — пайдаланушылар және компьютерлер» жабдығының көмегімен пайдаланушыларды құру. Бұл әдіс ең қолайлы болып табылады, өйткені түйсікпен түсінікті графикалық интерфейс пайдаланылады. Пайдаланушының құрылған есептік жазбасы атрибуттарының көпшілігін тапсыру үшін есептік жазбаны редакциялаудың құралдарын пайдалану керек. Пайдаланушылық есептік жазбаны құру үшін мынадай іс-қимылдарды орындау қажет:

1) «Active Directory — пайдаланушылар және компьютерлер» жабдығын ашу *(Басқару панелі/Жүйе және қауіпсіздік/Әкімшілендіру/Active Directory*— пайдаланушылар және компьютерлер;
2) Пайдаланушылық есептік жазба құрылатын бөлімшені таңдау (мысалы, *Developers* бөлімшеде). Бөлімше жабдықтың ағашынан таңдалады. Жаңа пайдаланушыны құру *Құру/Пайдаланушы* мәнмәтіндік мәзір командасының көмегімен жүргізіледі *(3.2-сурет);*
3) Пайда болған сұхбат терезесінде (3.3-сурет) құрылатын пайдаланушының атын, инициалын және тегін енгізу қажет.



3.2-сурет. «Active Directory — пайдаланушылар және компьютерлер» жабдығы арқылы жаңа пайдаланушыны құру



3.3-сурет. Пайдаланушылық есептік жазбаны құруға арналған сұхбат терезесі

Толық аты (домендегі бірегей) өрісі өздігінен толтырылады. *Пайдаланушының кіру аты* жолы пайдаланушының доменге кіруінің аты болып табылады. *Пайдаланушының кіру аты (Пред-Windows 2000)* өрісі алдыңғы ОС Windows 2000 жүйелеріне арналған кіру аты ретінде пайдаланылады. Өрістерді толтырғаннан кейін *Әрі қарай* батырмасын басу керек*;*

4) Пайдаланушының паролін енгізіп, оны растау керек. Бұл кезде:
   - жүйеге пайдаланушы бірінші рет кіргенде, өзінің есептік жазбасына арналған парольді дербес өзгерту тиіс екенін жүйеге көрсетуге болады;
   - *Пайдаланушының парольді өзгертуіне тыйым салу* опциясын таңдап, сіз пайдаланушыға өз пароліңізді ұсынасыз және оны өзгертуге тыйым саласыз;
   - *Парольдің әрекет ету мерзімі шектеусіз* опциясы парольдің әрекет ету мерзімі ешқашан аяқталмайтын және әр кез оны өзгертудің қажеті болмайтынын көрсетеді;
   - Егер *Есептік жазбаны тоқтату* опциясын таңдаса, онда осы есептік жазба оны қосқанға дейін әрі қарай жұмыс істеуге мүмкіншілік бермейтінін көрсетеді. Барлық атрибуттарды таңдау үшін *Әрі қарай* батырмасын басу керек*;*
5) Пайдаланушылық есептік жазбаны құру және шебердің жұмысы үшін *Дайын* батырмасын басу.

Шаблондарды пайдалану. Ұйымның бір құрылымдық бөлімшесінің пайдаланушыларының есептік жазбаларын басқару қолайлы болу үшін оларды шаблондардың негізінде арнайы бөлімшелерде құрған дұрыс.

Есептік жазбаның шаблоны — бұл барлық құрылған пайдаланушылар үшін ортақ атрибуттар алдын ала толтырылған есептік жазба. Пайдаланушының есептік жазбасының шаблонын құру үшін мынадай іс-қимылдарды орындау қажет:

1) пайдаланушының стандарттық есептік жазбасын құру. Ол үшін парольді енгізу бетінде *Есептік жазбаны тоқтату* жалаушаны орнату керек, өйткені бұл жазба шаблон ретінде ғана пайдаланылатын болады;
2) ұйымның осы құрылымдық бөлімшесінің барлық жазбалары үшін сәйкес келуге тиіс есептік жазбаның өрістерін редакциялап алу керек. Есептік жазба қасиеттерінің сұхбат терезесін шақыру мәнмәтіндік мәзір құралдарымен жүреді;
3) есептік жазбаның шаблоны үшін мәнмәтіндік мәзірдің көмегімен *Көшіру* командасын таңдау;
4) пайда болған сұхбат терезесінде *Объектіні көшіру — Пайдаланушы* пайдаланушының кіру атын және тегін енгізу;
5) келесі бетте парольді және растауды енгізу. Құрылған есептік жазба белсенді болу үшін *Есептік жазбаны тоқтату* опциясын тоқтату қажет. Осы кезеңде шебердің жұмысы аяқталады.

Командалық жолдың құралдарымен пайдаланушыларды құру. Командалық жолдың көмегімен пайдаланушылардың есептік жазбаларын құру үшін user модификаторы бар *Dsadd*c командасы пайдаланылады, ол құрылатын объектінің түрін көрсетеді. Параметр DN (Distinguished Name) объектінің атына жауап береді (әріптердің арасында бос орындар бар DN атын тырнақшаға алу керек). Осы командамен мынадай параметрлерді пайдалануға болады:

- *samid*— пайдаланушының есептік жазбасының аты;
- *upn*— пайдаланушының аты немесе алдыңғы Windows 2000 нұсқаларды пайдаланушының кіру аты;
- *fn*— пайдаланушының аты (жаңа есептік жазба құрудың шебері арқылы деректер толтыру кезіндегі *Аты* өрісі);
- *mi*— пайдаланушының инициалы;
- *ln*— пайдаланушының тегі;
- *display*— пайдалану интерфейсінде автоматты түрде құрылатын пайдаланушының толық аты;
- *empid*— пайдаланушы үшін құрылатын қызметкердің коды;
- *pwd*— пайдалану паролі (егер жұлдызша «*» символын көрсетсе, қарап шығудан қорғалған режимде пароль енгізу ұсынылады);
- *desc*— пайдаланушылық есептік жазба үшін қысқаша сипаттама;
- *memberof*— пайдаланушының бір немесе бірнеше топқа мүшелігін анықтайтын параметр;
- *office*— пайдаланушы жұмыс істейтін офистің орналасқан жері;
- *tel*— пайдаланушының телефон нөмірі;
- *email*— пайдаланушының электронды поштасының адресі;
- *hometel*— пайдаланушының үй телефонының нөмірі;
- *mobile*— пайдаланушының ұялы телефонының нөмірі;

- *fax*— факсимиле аппаратының нөмірі;
- *title*— пайдаланушының лауазымы;
- *dept*— пайдаланушы жұмыс істейтін бөлімнің атауы;
- *company*—компанияның атауы;
- *hmdir*— пайдаланушының құжаттары орналастырылатын негізгі каталог;
- *hmdrv*— есептік жазбаның үй папкасы орналастырылатын желілік дискіге апаратын жол;
- *profile*— пайдаланушының профилінің жолы;
- *mustchpwd*— жүйеге кейін кіру кезінде парольді ауыстыруға арналған параметр;
- *canchpwd*— парольді өзгертуге мүмкіншілік беретін параметр (егер параметрде «yes» көрсетілсе, онда пайдаланушының парольді ауыстыруына мүмкіншілік болады);
- *reversiblepwd*— кері шифрлауды қолданумен пайдаланушы паролінің сақталуына жауап беретін параметр;
- *pwdneverexpires*— парольді қолданыс мерзімі ешқашан таусылмайтынын көрсететін параметр;
- *acctexpires*— есептік жазбаның қолданыс мерзіміне (күндермен) жауап беретін параметр;
- *disabled*— есептік жазба тоқтатылғанын көрсететін пераметр;
- *q*— команданы өңдеуге арналған тыныш режимді көрсету.

Әрі қарай *DSadd* командасын пайдаланудың мысалы келтірілген*:*

Dsadd user cn="Иван I4BaHOB",OU=Developers,DC=ad,DC= example,DC=com -samid Ivan. Ivanov -upn Ivan. Ivanov -pwd * -fn Иван -ln Иванов -display "Иван Иванов" -tel "55555-55" -email Ivan. Ivanov@example. com -dept Әзірлеу -company Example -title Әзірлеуші -hmdir \\dc\profiles\ Ivan. Ivanov -hmdrv Z -mustchpwd yes -disabled no.

Кирил қарпі командалық жолда түзу көрсетілуі үшін, Юникодты орыс тілінде қолдамайтын бағдарламалардың тілін өзгерту қажет. Мұны басқару панелінің *Тіл және өңірлік стандарттар* тармағында жасауға болады.

PowerShell көмегімен пайдаланушыларды құру. Power- Shell ортасы — командалық жолдың қабығы, ол ОЖ деректерімен жұмыс істейтін ОЖ Windows және қосымшаларына әкімшілендіруді автоматтандыруға және басқаруға арналған. PowerShell командалық жолдың құралдарын қамтиды, олар *командлеттер* деп аталады.

Жаңа пайдаланушыны құру үшін Active Directory доменінде New-ADUser командлеті пайдаланылады. LDAP атын көрсету үшін *Path - параметрі* пайдаланылады, ол жаңа пайдаланушы үшін контейнер немесе бөлімше тапсырады. Егер бұл параметр тапсырылмаған жағдайда пайдаланушының объекті Users контейнерінде құрылады. Командлеттің параметрлері қауіпсіздік принципалының атрибуттарымен ұқсас.

Active Directory басқарумен байланысты командлеттерді пайдаланбас бұрын PowerShell үшін AD модулін орнатып, оны іске қосу қажет. Ол үшін Windows

PowerShell-де мынадай командаларды орындау керек:

```
import-module servermanager
Add-WindowsFeature -Name "RSAT-AD-PowerShell"
-IncludeAllSubFeature
import-module activedirectory
```

Әрі қарай New-ADUser командлетін пайдаланудың мысалы келтірілген:

```
New-ADUser-SamAccountName 'Ivan.Ivanov' -Name 'Иван Иванов' -GivenName
'Иван' -Surname 'Иванов' -DisplayName 'Иван Иванов' -Path 'OU=Developers,DC=ad,
DC=Example,DC=com' -CannotChangePassword $false -ChangePasswordAtLogon $true
-City 'Москва' -State 'Москва' -Country RU -Department 'Әзірлеу' -Title 'Әзірлеуші' -
UserPrincipalName 'Ivan. Ivanov@example. com' -EmailAddress
'ivan.ivanov@example.com' -Enabled $true -AccountPassword (Read-Host -
AsSecureString "AccountPassword")
```

Топтар құру. Пайдаланушыларды басқару қолайлы болу үшін және әкімшілендіру жүктемесін төмендету үшін кәсіпорындарда топтар объектілерін тартады. Топтар әр түрлі мақсаттарда пайдаланылады, оның ішінде: пайдаланушылар мен компьютерлердің Рөлдерін сәйкестендіру, қатынау рұқсаттары мен құқықтардың ерекше саясатын пайдалану, топтық саясатты сүзгіден өткізу және әкімшілендірудің өзге де міндеттері.

Active Directory-де топтардың екі түрін ажыратады: қауіпсіздік және тарату. *Қауіпсіздік топтары* SID-сәйкестендіргіштер бар қауіпсіздік принципалдарына жатады және қауіпсіздікті басқару үшін пайдаланылады. Топтардың бұл түрі ең жиі пайдаланылатын түрі болып табылады.

Тарату тобы электронды поштаны бірден барлық топқа жөнелту қолайлы болу үшін пайдаланушыларды топқа біріктіру қажет болған жағдайда Microsoft Exchange Server-ді орнатуға арналған. Қауіпсіздік топтарын сондай-ақ электронды поштаны тарату мақсатында да пайдалануға болады.

Топтың әрекет ету аймағын доменнің ішіндегі топ қолданылатын диапазон айқындайды. Топтардың әрекет ету аймағының негізгі сипаттамалары:

- топқа кіре алатын қауіпсіздік принципалдарын айқындайтын мүшелік;
- топтың репликация аймағын айқындайтын репликация;
- топтың тұрған жеріне жауап беретін қол жетімділік. Топтардың төрт әрекет ету аймағын ажыратады.

1. *Жергілікті топ.* Мұндай топтарға бір компьютерде ғана қатынауға болады, ACL тізілімінде пайдаланылады.
2. *Домендегі жергілікті топ.* Бұл аймақ ресурстарға қатынауға рұқсаттарды басқаруға арналған. Домендегі жергілікті топты доменнің кез келген қатардағы компьютерде кез келген ресурстың ACL тізіміне қосуға болады (Access Control List — қатынауды бақылау тізімі). Домендегі жергілікті топтарды әдетте бүкіл

домендегі қатынау ережелерін ұсыну үшін пайдаланады. Егер домен Windows NT деңгейінде немесе аралас деңгейде жұмыс істесе, онда мұндай топтар жергілікті топтар ретінде ғана пайдаланылатын болады.

3. *Жаһандық (глобальды) топтар.* Мұндай топтардың мүшелері болып пайдаланушылар және компьютерлер бола алады. Жаһандық топ бір доменнің ғана пайдаланушыларын, компьютерлерін және басқа жаһандық топтарды қамти алады. Бұл топтарды топтық саясаттардың әрекет ету аймағын сүзгіден өткізу үшін пайдалануға қолайлы. Жаһандық топтар өзінің доменінде де, сондай-ақ сенуші доменде де кез келген әмбебап және жергілікті топтардың мүшелері бола алады. Жаһандық топтарды доменде, орманда және сенуші домендегі ACL тізімдеріне қосуға болады.

4. *Әмбебап топ.* Мұндай топтар өзіне кіретін барлық ресурстарды басқару қолайлы болу үшін көптеген біріккен домендерден тұратын ормандарда жиірек пайдаланылады. Топтың әрекет ету аймағын топтар қасиеттерінің сұхбат терезесіндегі *Жалпылар* қосымша бетінде. Алайда топтардың әрекет ету аймақтарын мынадай жағдайларда өзгертуге болатынын ескеру керек:

- домендегі жергілікті топты әмбебап топқа, егер бұл топта доменде мүше ретінде басқа жергілікті топ болмаса;
- жаһандық топты әмбебап топқа, егер өзгертілетін топ басқа жаһандық топтың мүшесі болмаса;
- әмбебап топты жаһандық топқа, егер бұл топта мүше ретінде басқа әмбебап топ болмаса;
- әмбебап топты домендегі жергілікті топқа.

«Active Directory— пайдаланушылар және компьютерлер» жабдығының құралдары арқылы топтар құру. Бұл тәсіл ең қарапайым болып табылады, өйткені түйсікпен түсінікті графикалық интерфейстің құралдарымен жүзеге асырылады.

Жаңа топты құру үшін мынадай іс-қимылдарды орындау қажет:

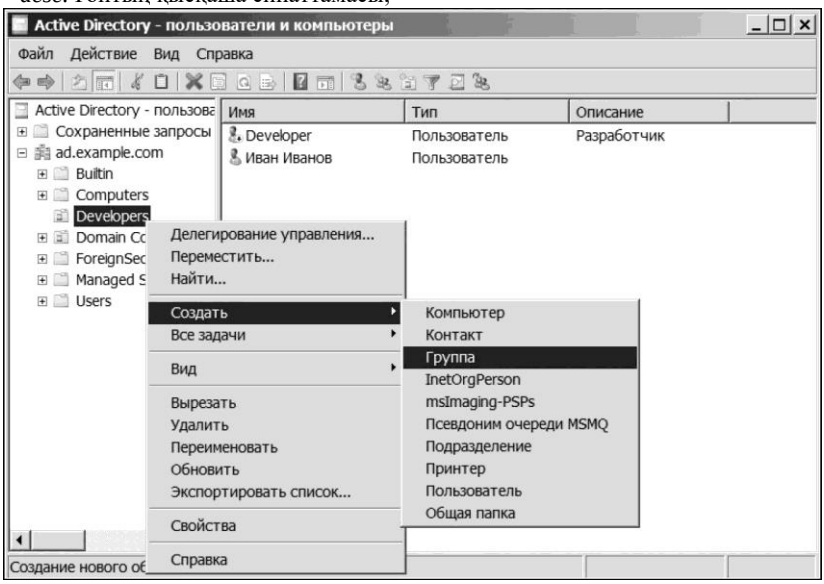
1) «Active Directory — пайдалануышылар және компьютерлер» жабдығын ашу *(Басқару паенлі / Жүйе және қауіпсіздік/Әкімшілендіру/ Active Directory— пайдаланушылар және компьютерлер*);
2) Топ құрылатын бөлімшеге өту. Бөлімшедегі мәнмәтіндік мәзірді шақырып, *Құру/Топ* командасын таңдау (3.4-сурет);
3) пайда болған *Жаңа объект — Топ* сұхбат терезесінде топтың атауын қосу. Сондай-ақ топтың түрін және топтың әрекет ету аймағын таңдау керек. Қажетті ақпаратты толтыру аяқталған соң, ОК батырмасын басу керек (3.5-сурет).

Командалық жолдың құралдарымен топтар құру. Пайдаланушылардың есептік жазбаларын құрғандай *group* модификаторымен *Dsadd*c командалық жолдың утилитасын пайдаланып, топтар құруға болады. Бұл команданың қосымша параметрлері мыналар болып табылады:

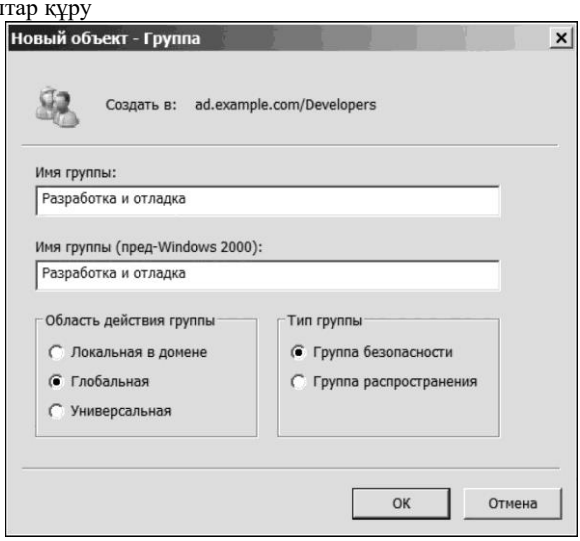
- *secgrp.* Үш топ: қауіпсіздік (yes) (үнсіз келісім бойынша) немесе тарату (no);
- *scope.* Топтың әрекет ету аймағы: домендегі жергілікті (l), жаһандық (g) (үнсіз

келісім бойынша) немесе әмбебап (u);

- *samid.* Осы топ үшін *samAccountName* бірегей атрибуты ретінде SAM атты пайдалануды айқындайды;
- *desc.* Топтың қысқаша сипаттамасы;



3.4-сурет. «Active Directory — пайдаланушылар және компьютерлер» жабдығының көмегімен топтар құру



- *memberof.* Жаңа топ қосу талап етілетін бір немесе бірнеше топты белгілейді (бірнеше топты бос орын арқылы қосу керек);
- *members.* Топқа мүшелерді қосу үшін пайдаланылады. Мүшелер DN-аттар түрінде көрсетілуі және бос орындар арқылы бөлінуге тиіс.

Пайдалануға арналған мысал:

```
Dsadd group cn="Әзірлеу және реттеу", OU=Developers,DC =ad,DC=example,
DC=com -secgrp yes -scope g -samid " Әзірлеу және реттеу " -desc " Әзірлеу және
реттеу бөлімшесі"
```

PowerShell құралдарымен топтар құру. PowerShell құралдарымен жаңа топ құру пайдаланушылардың есеп жазбаларын құрумен ұқсас. Active Directory доменінде жаңа топ құру үшін *New-ADGroup командлеті пайдаланылады.* Параметр — *GroupCategory* топтың түрін көрсетеді. Параметр — *GroupScope* топтың әрекет ету аймағын көрсетуге арналған. Параметр — *DisplayName* топтың бейнеленетін атына жауап береді, ал — *SamAccountName* — алдыңғы Windows 2000 аты.

Командлет мынадай қалыпта көрсетіледі:

```
New-ADGroup [-Name] [-GroupScope] [-AuthType { | }] [-Credential ] [-Description ]
[-DisplayName ] [-GroupCategory ] [-HomePage ] [-Instance ]
[-ManagedBy ] [-OtherAttributes ] [-PassThru ] [-Path ] [-SamAccountName ] [-Server ]
[-Confirm] [-WhatIf] []
```

Пайдалану мысалы:

```
New-ADGroup -Name "Бағдарламашылар" -SamAccountName "Бағдарламашылар" -
GroupScope Global -GroupCategory Security -Description "Бағдарламашылар
командасы" -Path "OU=Developers, DC=ad,DC=example,DC=com"
```

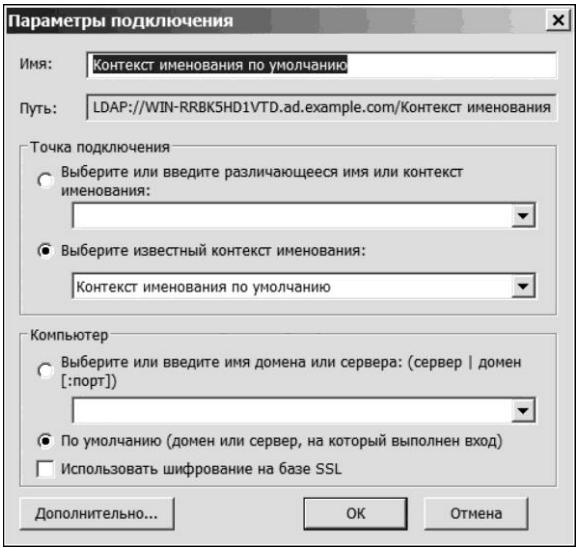
Топтағы мүшелікті басқару. Деректерге қатынауды басқару үшін каталогтарға қатынаудың жеңілдетілген хаттамасын, пайдаланушылар мен топтарды пайдаланады. Каталогтарға қатынаудың жеңілдетілген хаттамасы Windows пайдаланушылары мен Active Directory пайдаланушыларын және олардың Active Directory топтарындағы мүшелігін бір мезгілде пайдалануын қолдайды.

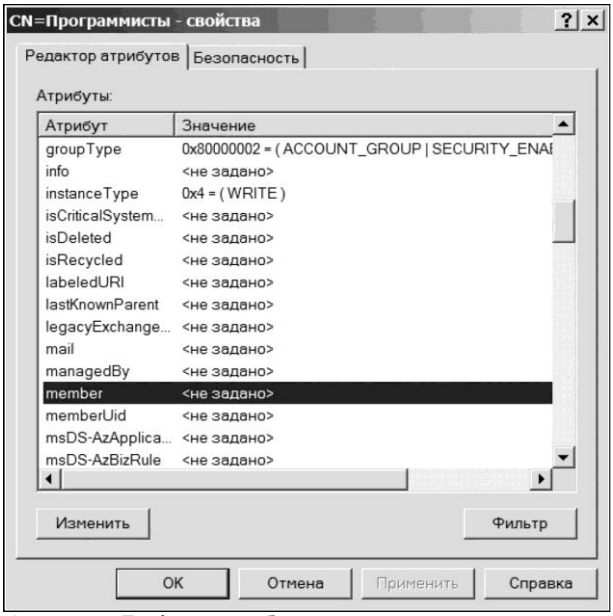
Active Directory деректеріне қатынауды ұсыну және бақылау процедураларын орындау үшін AD LDS данасының «Әкімшілер» тобына жату қажет. AD LDS баптау кезінде AD LDS әкімшісі ретінде көрсетілген пайдаланушы «Әкімшілер» тобының мүшесі болады.

AD LDS тобының мүшелерін қосу немесе жою үшін мынадай іс-қимылдарды орындау:

1) *Бастау* мәзірінде *ADSI Әкімшілендіру/Редакциялау тармағын таңдау;*
2) консольдің ағашында *Редакциялау ADSI элементін таңдап, мәнмәтіндік мәзірдің көмегімен Іс-әрекет/ Қосу... командасын таңдау;*

3) қосу параметрлері бар сұхбат терезесі ашылады (3.6-сурет). *Ат* өрісі қосудың белгісіне жауап береді. *Таңдаңыз немесе доменді немесе немесе серверді енгізіңіз* өрісінде AD LDS керекті данасы орындалатын DNS-атын, NetBIOS-атын немесе компьютердің IP-адресін, сондай-ақ AD LDS данасын пайдаланатын LDAP портының нөмірін енгізу қажет. *Қосу нүктесі* бөлімінде оған қосылу талап етілетін атты немесе атаудың мәтінін таңдау керек. Параметрлерді енгізгеннен кейін, OK батырмасын басу керек;
4) түрлендіру талап етілетін AD LDS данасының каталогына қосуды және байлауды орындау;





3.7-сурет. Бөлімше атрибуттарының редакторы

5) консольдің ағашында каталогтың өзгерту талап етілетін топ бар бөліміне кіру және мәнмәтіндік құралдармен редакцияланатын топтың қасиеттеріне кіру керек;
6) *Атрибуттар* тізімінде *Мүше* элементін таңдап, *Өзгерту* (3.7-сурет) батырмасын басу. *Қауіпсіздік қатысушыларының көп мәнді ажыратылатын аттарының редакторы* құралымен топтың қатысушыларын топқа қосу;
7) *Қауіпсіздік қатысушыларының көп мәнді ажыратылатын аттарының редакторы* құралында топтан қатысушыларды жою үшін топтан жойылатын топтың әрбір мүшесі үшін *Жою* батырмасын басу керек.

AD LDS пайдаланушылардың есептік жазбаларын ажырату немесе қосу. AD LDS пайдаланушылардың есептік жазбаларын ажырату немесе қосу оның AD LDS каталогқа байлауды жүзеге асыру қабілетіне әсер етеді. AD LDS пайдаланушылардың есептік жазбаларын ажырату немесе қосу үшін «PADSI редакциялау» жабдығы пайдаланылады.

PowerShell құралдарымен топтармен жұмыс. PowerShell топтармен және олардағы мүшелікпен жұмыс істеу мүмкіншілігін ұсынады, бұл осы процесті автоматтандыруды мүмкін етеді, мысалы, жаппай айла-шарғы жасау кезінде. Топтардағы мүшелікті басқаруға арналған негізгі командлеттер мыналар:
Get-QADGroupMember— топ мүшелерін алу: Get-QADGroupMember DomainName\Developers

Add-QADGroupMember— объектіні топқа қосу:
Add-QADGroupMember DomainName\Developers -Member DomainName\Ivanov
Remove-QADGroupMember— топтан алып тастау:
Remove-QADGroupMember DomainName\Developers -Member DomainName\Ivanov
Жаппай қосу қажет болғанда келесі команданы пайдалануға болады:
Get-QADUser-Title Developer | Add-QADGroupMember DomainName\Developers
Алдыңғы командағы сүзгішті қосқан кезде, мысалы, қандайда бір критерий бойынша жауап беретін әзірлеушілерді ғана қосуға болады:
Get-QADGroupMember DomainName\Developers | where {$. Country -eq "Russia"} | Add-QADGroupMember DomainName\ Russia Developers
Топтағы мүшелікті көшірмелеу үшін төмендегі команданы пайдалануға болады:
Get-QADGroupMember DomainName\Developers | Add- QADGroupMember DomainName\Developers New
PowerShell құралдарымен топтардағы мүшелікпен жаппай операцияларды пайдаланудың түрлі нұсқалары, оның ішінде PowerShell шарттары мен басқа да мүмкіндіктерін пайдаланатын нұсқалары болуы мүмкін.4.

3. 4. ТОПТЫҚ ДОМЕН САЯСАТЫН БАПТАУ

Топтық саясат — бұл пайдаланушы мен компьютерлер параметрлерінің көптеген жиынтығын бір уақытта конфигурациялауға мүмкіндік беретін инфрақұрылым болып табылатын Active Directory домендік қызметі негізінде Windows ортасын баптау құралы. Топтық саясаттар домен ішінде құрылады. Топтық саясаттың параметрлері топтық саясаттар объектілерінің (Group Policy Object — GPO) құрамында болады. Топтық саясаттың объектілері Active Directory каталогтар қызметінің контейнерлерімен байланысады. GPO объектілерді Active Directory каталогтар объектілеріне жоспарлы пайдалану тиімді әрі жеңіл басқарылатын компьютерлік жұмыс ортасын құруға мүмкіндік береді. Саясат Active Directory каталогының иерархиясы бойынша жоғарыдан төмен қолданылады. Топтық саясат параметрлерін де әр комьютерде жергілікті баптауға болады, алайда жергілікті топтық саясатты Active Directory домендік қызметі негізінде пайдалануға кеңес берілмейді, себебі бұл жағдайда әр компьютерді жеке-жеке баптау талап етіледі.

Топтық саясаттарды пайдалануды басқару. Топтық саясаттарды басқару топтық саясаттарды басқару консолі арқылы іске асырылады. Оны ***Қосу: Әкімшілендіру/Топтық саясатты басқару*** мәзірінің тармағы арқылы іске қосуға болады. Топтық саясаттарды басқару консолі топтық саясат объектілерін құру, жылжыту және жою үшін пайдаланылады. Доменнің топтық саясатының барлық объектілері топтық саясаттарды басқару консолінің топтық саясаттар

объектілерінің бумасында көпшілікке қол жетімді.

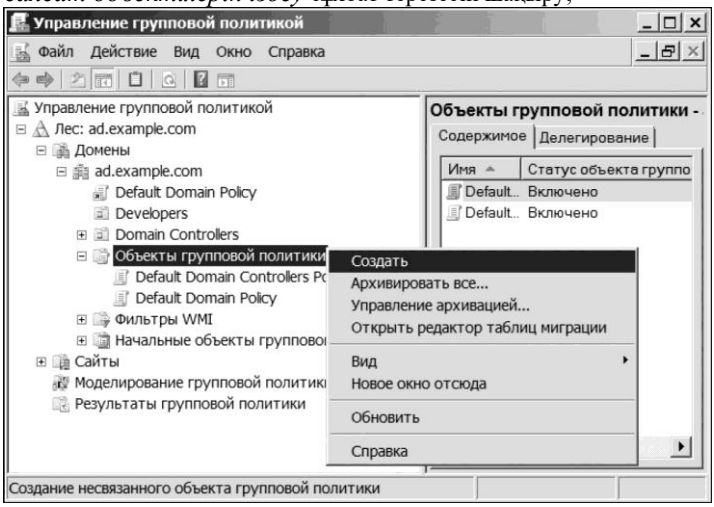
Үнсіз келісім бойынша топтық саясаттың екі объектісі құрылады. *Default Domain Controller Policy* құрамында домен бақылаушыларына қолданылатын саясаттар параметрлері бар. *Default Domain Policy* құрамында домендегі барлық компьютерлер мен пайдаланушыларға қолданылатын саясаттар параметрлері бар.

Топтық саясаттар объектісін құру. Топтық саясаттардың жаңа объектісін құру үшін мына іс-әрекеттерді орындау қажет:

1) Топтық саясат жабдығында редакцияланатын доменнің *Топтық саясат объектілері* контейнерін таңдау. Осы контейнердің мәнмәтіндік мәзір құралдары арқылы *Құру* командасын таңдау (3.8 -суреті);
2) Пайда болған *Топтық саясаттың жаңа объектісі* сұхбат терезесінде объектінің атауын *«Аты»* өрісіне енгізіп, ОК батырмасын басу.

Топтық саясат объектілерін іздеу. Топтық саясаттарды басқару консолінің құралдары топтық саясат объектілерін іздеп табуға мүмкіндік береді. Топтық саясат объектісін табу үшін мынадай іс-әрекеттерді орындау қажет:

1) «Топтық саясатты басқару» жабдық консолінің ағашынан орман немесе доменді таңдау және *Табу* мәнмәтіндік мәзір командасы арқылы *Топтық саясат объектілерін іздеу* сұхбат терезесін шақыру;



3.8-сурет. Топтық саясаттың жаңа объектісін құру

2) *Топтық саясат объектілерін іздеу* сұхбат терезесінде іздеу салынатын доменді таңдау. Ол үшін *Топтық саясат объектілерін доменнен іздеу* элементін пайдалану қажет*;* ашылған *Іздеу элементі* тізімінде іздеу орындалатын объектінің типін таңдау; *Шарт* тізімі іздеу салу үшін шарт («Құрамында бар», «Құрамында жоқ» және «Сәйкес келеді») қоюға мүмкіндік береді; *Мән* өрісі іздеуді сүзгіден өткізу үшін пайдланылады (3.9-сурет);
3) Іздеу шарттарын таңдау үшін *Қосу* батырмасын басу*;*

4) *Табу* батырмасын басу, бұдан кейін іздеу нәтижелерімен танысуға болады.

Топтық саясат объектісін жою. Топтық саясаттың объектісін мыналардың көмегімен жоюға болады:

- *Топтық саясатты басқару* сұхбат терезесіндегі *Жою* батырмасы;
- құрал-саймандар панеліндегі *Жою* батырмасы;
- топтық саясат объектісінің мәнмәтіндік мәзірінің *Жою* тармағы.

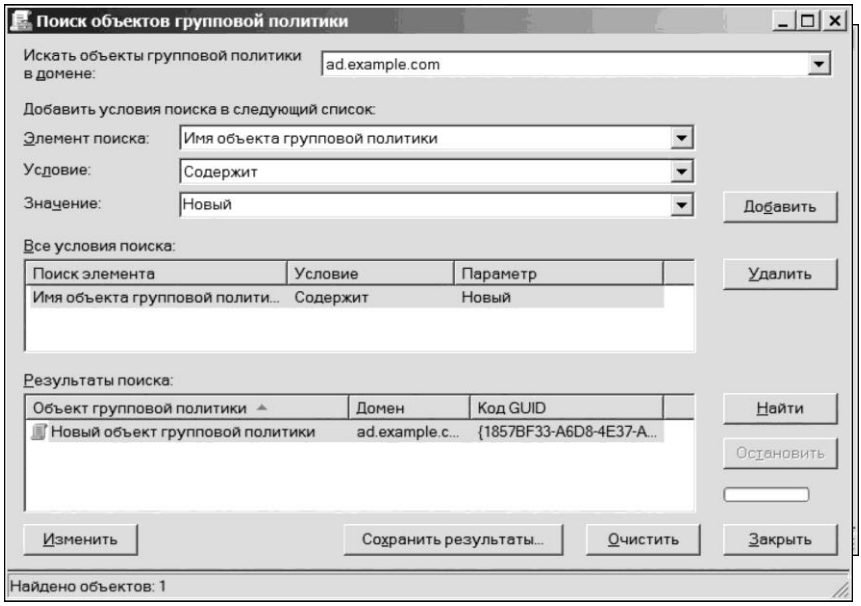
Топтық саясат байланыстары. Топтық саясат объектілері әсер тигізуі үшін оларды контейнермен байланыстыру керек. Бұл жағдайда топтық саясат байланысқан контейнердегі компьютерлер мен пайдаланушыларға осы топтық саясат объектісінің параметрлерін қолданады. Топтық саясаттың бір объектісін бір уақытта бірнеше құрылымдармен, домендермен және сайттармен байланыстыруға болады.

Топтық саясаттың *қолданыстағы объектісін* байланыстыру үшін:

1) *Топтық саясатты басқару* консолінде топтық саясаттың қолданыстағы объектісімен байланыс құруды талап ететін құрылым, домен немесе сайтты таңдау;
2) мәнмәтіндік мәзір құралдары арқылы *Топтық саясаттың қолданыстағы объектісін байланыстыру* командасын таңдау және пайда болған *Топтық саясат объектісін таңдау* сұхбат терезесінде топтық саясат объектісін белгілеп, ОК батырмасын басу қажет.

Топтық саясаттың *қолданылмайтын объектісін* байланыстыру үшін:

1) *Топтық саясатты басқару* консолінде топтық саясаттың қолданыстағы объектісімен байланыс құруды талап ететін құрылым, домен немесе сайтты таңдау;



2) мәнмәтіндік мәзір құралдары арқылы *Осы доменде топтық саясат объектісін құру және оны ... байланыстыру* командасын таңдау және пайда болған *Топтық саясаттың жаңа объектісі* сұхбат терезесінде жаңа объектінің атын енгізіп, ОК батырмасын басу қажет. Сондағы ары қарай баптауды талап ететін жаңа объекті құрылады.

Топтық саясатты мұралану және топтық саясаттардың басымдылықтары. Топтық саясат объектісін құрылымдармен байланыстырған кезде топтық саясаттың осы объектісі барлық еншілес құрылымдардың барлық компьютерлері мен пайдаланушыларына қолданылады.

Топтық саясат басымдылықтары топтық саясат объектілерін өңдеу тәртібін көрсету есебінен топтық саясат параметрлерінің қақтығысын болдырмау үшін пайдаланылады. Басымдылығы жоғары топтық саясат объектілері басымдылығы төмен объектілерге қарағанда артықшылықтарға ие.

Таңдалған контейнер үшін *Топтық саясатты мұралану* қосымшасындағы *Топтық саясатты басқару* консолінен топтық саясат басымдылықтарын қарауға болады.

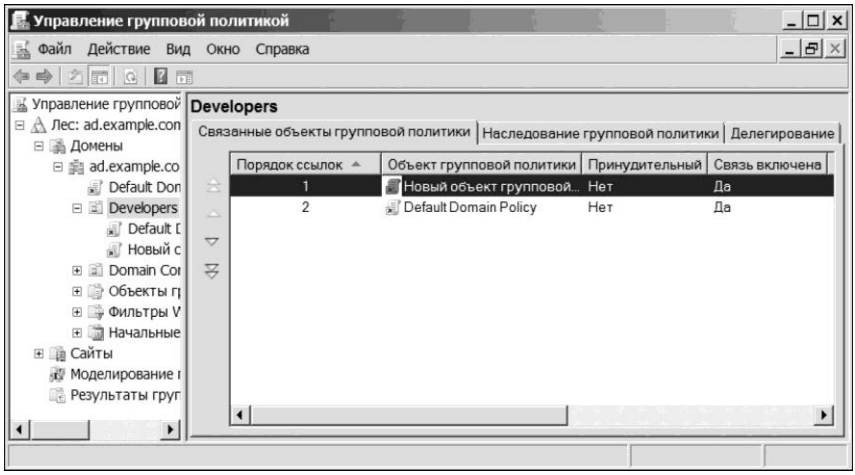
Топтық саясат параметрлері мына тәртіпте қолданылады:

1) жергілікті компьютерлерде орналасқан топтық саясаттың жергілікті объектілері;
2) Active Directory сайтының деңгейіндегі топтық саясат объектілері;
3) Active Directory доменінің деңгейінде белгіленген топтық саясат объектілері;
4) құрылым деңгейіндегі топтық саясат объектілері.

Топтық саясатты пайдалану тәртібін өзгертуге болады. Ол үшін мынадай іс-әрекеттер орындау қажет:

1) Топтық саясат басымдылықтарының тәртібін өзгертуге талап қойылатын *Топтық саясатты басқару* консолінің ағашынан доменді таңдау;
2) Топтық саясаттың байланысқан объектілері қосымшасында басымдылығын өзгертуге талап қойылған топтық саясат объектісін таңдау және басымдылығын өзгерту үшін *Байланысты жоғары жаққа жылжыту* немесе *Байланысты оң жақ орынға жылжыту* батырмаларының бірін пайдалану (3.10-сурет).

Топтық саясат объектілерін редакциялау. Топтық саясат объектілерін редакциялау үшін Топтық саясаттарды басқару консолінің топтық саясат объектісіне мәнмәтіндік мәзір құралдары арқылы *(Өзгерту* мәнмәтіндік мәзір командасын таңдау қажет*)* шақыртатын «Топтық саясаттарды басқару редакторы» жабдығын пайдалану керек.



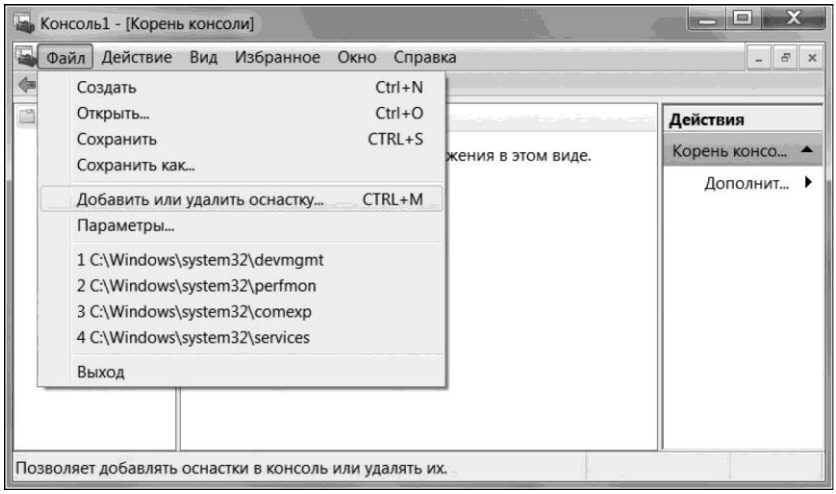
3.10-сурет. *Developers бөлімшесінің топтық саясаттарын қолдану тәртібін өзгерту*

Қауіпсіздік шаблонын құру және оны топтық саясатпен бірге пайдалану. *Қауіпсіздік шаблоны* — бұл қауіпсіздік конфигурациясын басқарудың иілгіш механизмі. Ол өз алдына inf кеңейтілуі бар мәтіндік файл болып табылатын және құрамында қауіпсіздік конфигурациясы параметрлерінің жиынтығы бар.

Қауіпсіздік шаблондары қауіпсіздіктің келесі құрамдас бөліктерін баптауға мүмкіндік береді: жергілікті саясат; есептік жазбалар саясаты; оқиғалар, топқа қол жетімділігін шектеу журналдары; жүйелік қызметтер конфигурациясы; жүйелік тізілімге қол жетімділігін беру; файлдық жүйелердің қауіпсіздігін баптау және т.б.

«Қауіпсіздік шаблондары» жабдығы. Осы жабдықты іске қосу үшін мына іс-әрекеттерді орындау қажет:

1) *Қосу Стандарттық/Орындау* (немесе Win + R пернелерінің комбинациясы арқылы) мәзірі тармақтарының құралдары арқылы MMC басқару консолін ашу және *Ашу* өрісіне *mmc* енгізіп, ОК батырмасын басу;
2) *Файл/Жабдықты қосу немесе жою* мәзірінің тармағын таңдау немесе Ctrl + M пернелерінің комбинациясын пайдалану(3.11-сурет); пайда болған *Жабдықты қосу немесе жою* сұхбат терезесінде *Қауіпсіздік шаблондары* жабдығын таңдап, *Қосу* батырмасын басу, бұдан кейін ОК батырмасын басу. Құрылатын



3.11-сурет. ММС басқару консолі

қауіпсіздік шаблондары / *Documents/Security/Templates/* папкасында сақталатын болады.

Жаңа қауіпсіздік шаблонвн құру. Жаңа қауіпсіздік шаблонын құру үшін келесі іс-әрекеттерді орындау қажет:

1) консоль ағашында «Қауіпсіздік шаблондары» жабдығын бірінші реті іске қосқанда автоматты түрде құрылатын *%Userprofile%/\Documents/ Security/Templates/*(үнсіз келісім бойынша) торапты таңдау;
2) мәнмәтіндік мәзірдің құралдары арқылы консольдің белгіленген элементінен *Шаблон құру* командасын таңдау;
3) пайда болған сұхбат терезесіндегі *Шаблонның аты* мәтіндік өрісіне жаңа шаблонның атын және *Сипаттау* өрісіне шаблон мақсатының сипаттамасын енгізу

Қауіпсіздік шаблондарының консолінде құрылған қауіпсіздік шаблонын бейнелеу 3.12-суретте келтірілген.

Қауіпсіздік шаблондарын қарапайым мәтіндік редакторлармен редакциялауға болады. Бұдан бұрын көрсетілгендей, қауіпсіздік шаблондарының файлын *%Userprofile%/Documents/ Security/Templates/* папкасынан табуға болады.

Қауіпсіздік шаблонының баптауларын конфигурациялау. Өз алдына, қауіпсіздік шаблондарының жабдығы топтық саясаттар жинағының редакторы ғана болып табылады. Жаңа қауіпсіздік шаблонын құрғаннан кейін консольде топтық саясаттар пайда болады. Алайда бұндай жабдықтау жұмыс ортасының ағымдағы конфигурациясының өзгеруіне әсер етпейді.

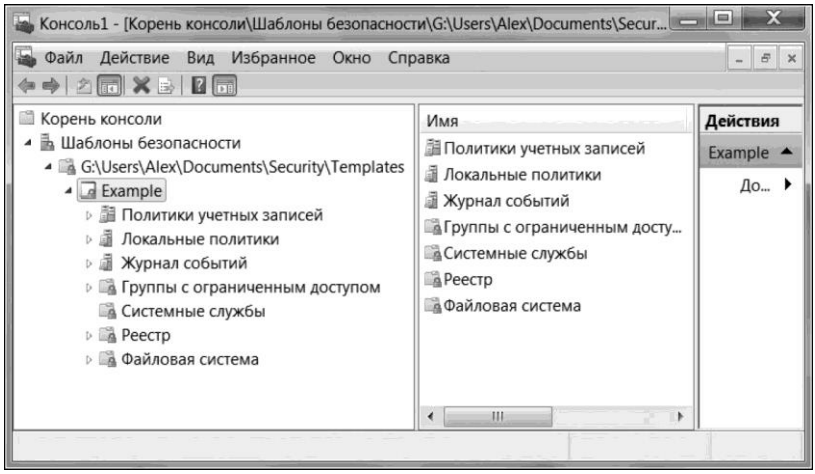
Қол жетімділігі шектеулі топтарды баптау. Қауіпсіздік шаблонының осы бөлімі қандай да бір топқа жататын пайдаланшыларды анықтауға мүмкіндік береді. Сондағы қауіпсіздік шаблондарымен бірге пайдаланылатын саясаттар осы топқа

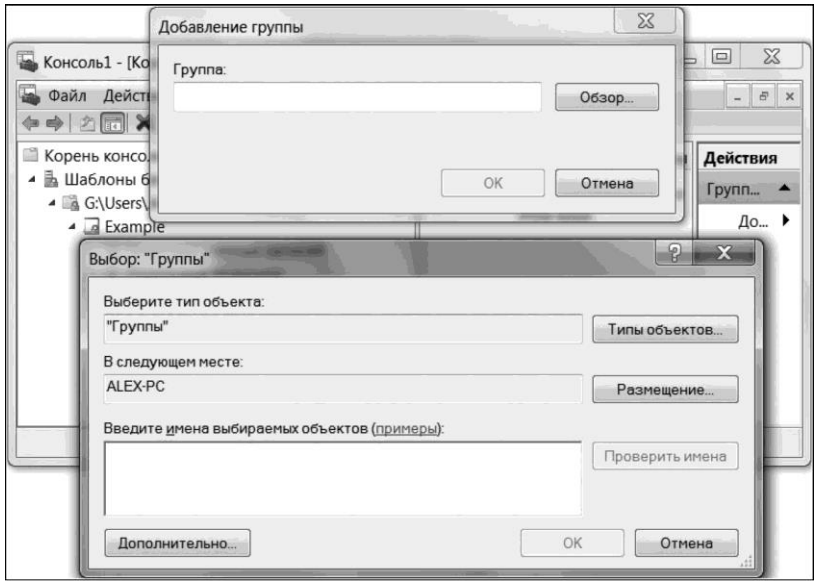
кіретін барлық пайдаланушыларға таралатын болады.

Қол жетімділігі шектеулі топтардың мүшелерін қосу үшін келесі іс-әрекеттерді орындау қажет:

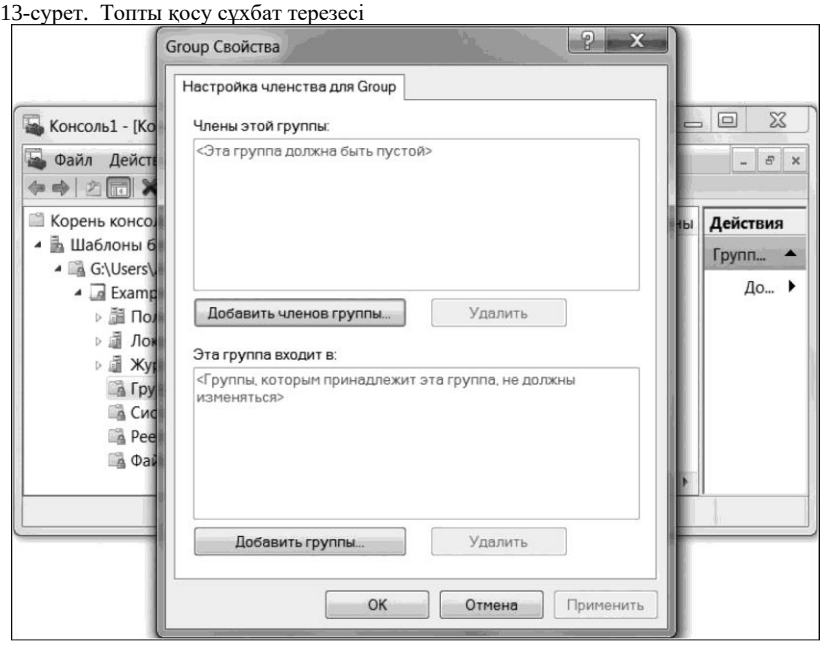
1) қауіпсіздік шаблондарының консолінде *Қол жетімділігі шектеулі топтар* элементін белгілеу және *Топты қосу* командасын таңдап, мәнмәтіндік мәзір құралдары арқылы жаңа топты қосу;
2) Пайда болған *Топты құру* сұхбат терезесінде жаңа топтың атын енгізу немесе *Шолу* батырмасын қолдана отырып, қолданыстағы топты табу (3.13-сурет);
3) ОК батырмасын басу, жаңа топтардың қасиеттері сұхбат терезесі шығады, оның көмегімен осы топтың пайдаланушыларын қосуға, сонымен қатар бас топты таңдауға болады (3.14-сурет);
4) ОК батырмасын басу, жаңа топ құрылады және «Қауіпсіздік шаблондары» жабдығының қол жетімділігі шектеулі топтар торабында пайда болады.

Жүйелік қызметтерді баптау. Қауіпсіздік шаблондар жабдығының *Жүйелік қызметтер* торабы топтық саясат құралдары арқылы жүйелік қызметтер конфигурациясын өзгертуге арналған. Қауіпсіздік шаблондар құралы арқылы жүйелік қызметтерді конфигурациялау





3.13-сурет. Топты қосу сұхбат терезесі



бір уақытта бірнеше компьютерлерде жүйелік қызметтерді баптауға мүмкіндік береді.

Қауіпсіздік шаблондарының құралдары арқылы жүйелік қызметтерді конфигурациялау үшін мынадай іс-әрекеттерді орындау қажет:

1) Қауіпсіздік шаблондарының консолінде *Жүйелік қызметтер* торабын таңдау;
2) Баптауды жоспарлап отырған іске қосудың қызметін, типін таңдау. Дискіні дефрагменттеу қызметін іске қосуға тыйым салынсын ;
3) Мәнмәтіндік мәзір құралдары арқылы бапталатын қызметтер қасиеттерін ашу;
4) Пайда болған *Қасиеттер: Дискіні дефрагменттеу* сұхбат терезесінде *Шаблондағы келесі қызмет параметрлерін анықтау* опциясын таңдау және *Тыйым салынған* тармағында ауыстырып қосқышты орнату. ОК батырмасын қосу арқылы қасиеттерге енгізілген өзгертулерді растау.

Жүйелік тізілімді баптау. Осы торапты пайдалану қауіпсіздік шаблон құралдары арқылы жүйелік тізілімге және оның жеке элементтеріне қол жетімділігін баптауға мүмкіндік береді. «Тұтынушылар» тобының барлық мүшелеріне тізілімге қол жетімділігіне толық тыйым салу тапсырмасы тұрсын. Бұл үшін мынадай іс-әрекеттерді орындау қажет:

1) Қауіпсіздік шаблондарының консулінде *Тізілім* торабын таңдау;
2) Таңдау жасалған торапқа мәнмәтіндік мәзір құралдары арқылы *Бөлім қосу* командасын таңдау*;*
3) Пайда болған *Тізілім бөлімін таңдау* сұхбат терезесінде [CLASSES_ROOT] бөлімін таңдау немесе *Таңдалған бөлім* өрісіндегі бөлімге жол енгізіп, ОК батырмасын басу;
4) Пайда болған сұхбат терезесінде *Тұтынушылар* тобына тыйым қойып, ОК батырмасын басу;
5) *Объектіні қосу* сұхбат терезесінде осы қауіпсіздік баптауларын кеңінен барлық еншілес құрылымдарға тарату, көрсетілген бөлімдегі рұқсаттарды ауыстыруға тыйым салу немесе параметрлерді қолмен өзгерту. ОК батырмасын басқанда осы өзгертулер «Қауіпсіздік шаблондары» жабдығының *Тізілім* торабында көрсетілеті болады;
6) [MACHINE] және [USERS] тізілімінің бөлімдері үшін 3 – 5 тармақтарындағы іс-әрекеттерді жасау.

Файлдық жүйені баптау. Файлдарға жол сілтеуге қауіпсіздік параметрлерін алу үшін мынадай іс-әрекеттерді орындау қажет:

1) «Қауіпсіздік шаблондары» жабдығында *Файлдық жүйе* торабын белгілеу және осы торап үшін мәнмітіндік мәзір құралдары арқылы *Файлды қосу* командасын таңдау*;*
2) Пайда болған *Файл немесе папканы қосу* сұхбат терезесінде файл немесе папкаға бағыт сілтеу;
3) *...үшін деректер қорының қауіпсіздігі* сұхбат терезесінде пайдаланушалар мен топтарға рұқсат алып, ОК батырмасын басу;
4) Пайда болған *Объектіні қосу* сұхбат терезесінде рұқсатты ауыстыруға тыйым салу немесе рұқсатты баптау;
5) Баптауды аяқтау үшін ОК батырмасын басу.

Барлық файлдар мен папкаларға енгізілетін рұқсаттарды тарату опциясы

барлық еншіленген рұқсаттарды осы бағытқа, сонымен қатар ішіне салынған барлық жолдарға қолдануға мүмкіндік береді. Қолданыстағы рұқсаттар осы бөлімге арналған қауіпсіздік рұқсаттарының жиынтығымен қақтығысқа шыққан кезде ғана ауыстырылады. *Барлық бағыңқы папкалар мен файлдарға арналған қолданыстағы рұқсаттарды еншіленген рұқсаттарға ауыстыру* опциясы осы жолдар, сонымен қатар оның ішіне салынған барлық бағыттар үшін барлық қолданыстағы рұқсаттарды ауыстыруға мүмкіндік береді. Барлық қолданыстағы рұқсаттар жойылып, ағымдағылар ғана қалады.

Қауіпсіздік шаблонын сақтау. Қауіпсіздік шаблонын өзгертіп біткен соң, оны ары қарай пайдалану үшін сақтау қажет.

Қауіпсіздік шаблонын сақтау үшін мәнмәтіндік мәзір құралдары арқылы қауіпсіздік шаблонының торабы үшін *Сақтау* немесе *...ретінде сақтау* командасын таңдау қажет.

Қауіпсіздік шаблондарын ашу. Қауіпсіздік шаблондары доменнің ішінде Active Directory топтық саясат объектілерінің көмегімен ашылуы мүмкін. Бұл үшін саясатты жаңартқаннан кейін топтық саясаттың таңдалған объектісінің іс-әрекет ететін саласындағы барлық компьютерлері талап етілетін қауіпсіздік параметрлерін алуы үшін қауіпсіздік шаблонын топтық саясат объектісіне импорттауға талап қойылады. Қажет болған жағдайда түрлі типтегі компьютерлерге бөлімше құрып, кейін олардың ішіне осы компьютерлердің есептік жазбаларын орналастыруға болады.

Қауіпсіздік шаблонын топтық саясат объектісінде ашу үшін мынадай іс-әрекеттер орындау қажет:

1)арнайы құрылған объектіні Active Directory құрылымының белгілі деңгейімен байланысқан топтық саясаты арқылы ашу және топтық саясат редакторының құралдары арқылы К*омпьютер конфигурациясы /Windows конфигурациясы/Қауіпсіздік параметрлері* торабын ашу;

2) Ашылған торап үшін мәнмітіндік мәзір құралдары арқылы *Саясат импорты* командасын таңдау;

3) Пайда болған ... *импорттау саясаты* сұхбат терезесінде қауіпсіздік шаблонын таңдап, *Ашу* батырмасын басу.

3.5. АҚПАРАТТЫ ҚАУІПСІЗ ТАБЫСТАУҒА КОНФИГУРАЦИЯЛАУ

IPsec хаттамаларын пайдалану. IPsec (Internet Protocol security) — желіаралық IP хаттамасы бойынша берілетін деректердің қорғауын қамтамасыз ететін хаттамалар жиынтығы. IP желілері бойынша деректерді жасырын беру стандарты болып табылады және шынайылығын растау, тұтастығын тексеру және (немесе) IP-пакеттердің шифрленуін жүзеге асыруға мүмкіндік береді. IPsec құрамына Интернеттегі кілттермен қорғалып алмасуға арналған хаттамалар да енеді. Көбінесе VPN-қосылуларды (Virtual Private Network) ұйымдастыру үшін пайдаланылады.

Virtual Private Network (виртуалды дербес желі) — басқа желінің үстінен бір немесе бірнеше желілік қосылуларды қамтамасыз етуге мүмкіндік беретін технология.

интернет көпшілікке қол жетімді болып, белсене дами бастағанда IPsec пайда болды. Қорғалған хаттамаларды құру қажеттілігі пайда болды. Себебі қауіпсіздік бөгде тұлғалардан объектілерді физикалық оқшаулау деңгейінде ұйымдастырылды. Желіге Қол жетімділігін машиналардың шектеулі саны иемделді. 1994 жылы Интернеттер сәулеті бойынша кеңес (IAB) «Интернеттер сәулетінің қауіпсіздігі» есебін жарыққа шығарды. Ол қазіргі уақытта да қолданылатын RFC2401—RFC2412 қорғалған хаттамалар стандарттарын құруға алғышарт болып табылады.

IPsec - IPv6-хаттамасының бөлігі немесе IPv4 хаттамасының кеңейтілімі болып табылады. IPsec желі деңгейінде (ISO/OSI моделіндегі 3-ші деңгей) орналасады (3.1-кесте). Ол осы деңгейдің ең кең таралған IP хаттамасын пайдаланады және бұл оны иілгіш етеді. TCP/IP хаттамалар отбасында негізделетін кез келген хаттамаларды қорғау үшін пайдаланылуы мүмкін және қолданыстағы қосымшалар мен ОС өзгерістер енгізуді талап етпейді.

Көп жағдайда IPsec хаттамасы жаңа құрал-жабдықтарды орнатуды немесе ескіні ауыстыруды қажет етпейді. Бұл оны енгізудің құнын төмендетеді. Хаттама стандартқа сай және ашық болып табылады және де барлық дерлік заманауи ОС қамтамасыз етіледі. Осылайша, бұл хаттама деректердің құпия сақталуына

3.1-кесте

TCP/IP деңгейі	ISO/OSI деңгейі
4. Қолданбалы бағдарламалар	7. Қолданбалы бағдарламалар 6. Деректерді ұсыну
3. Көліктік	5. Сеанстық 4. Көліктік
2. Желіаралық	3. Желілік
1. Желіге қол жеткізу	2. Арналық 1. Физикалық

және желілік жабдыққа қосымша шығынсыз пайдаланушылардың шынайылығын бұдан бұрын қорғалмаған желіде тексеруді қамтамасыз етуге мүмкіндік береді. Сонымен қатар криптографияға негізделген қызметтердің көмегімен қауіпсіздіктің жоғары бапталатын деңгейін қамтамасыз етеді.

IPsec жиынтығына үш хаттама енеді:

1) *Authentication Header* (AH) — виртуалды қосылулардың тұтастығын, ақпарат көзінің сәйкестендірілуін және қайтадан пакеттер берілімін болдырмау атқарымын қамтамасыз етеді;
2) *Encapsulating Security Payload* (ESP) — жіберілетін ақпараттың құпиялығын, жасырын трафик тасқынының кемуін қамтамасыз етеді;
3) *Internet Security Association and Key Management Protocol* (ISAKMP) — қосылуды алғашқы баптау, бірін-бірі соңғы түйіндермен өзара сәйкестендіру және құпия кілттермен алмасу үшін пайдаланылатын хаттама.

Authentication Header және Encapsulating Security Payload хаттамалары мейлінше қолайлы қауіпсіздік деңгейін қамтамасыз ету үшін бірігіп, сонымен қатар бір-біріне тәуесіз пайдаланылуы мүмкін.

IPsec хаттамасының жұмысы екі режимде мүмкін болады: көліктік және туннельдік. Әр түрлі режимде IPsec жиынтығына кіретін хаттамалар атқарымының айырмашылығы болады.

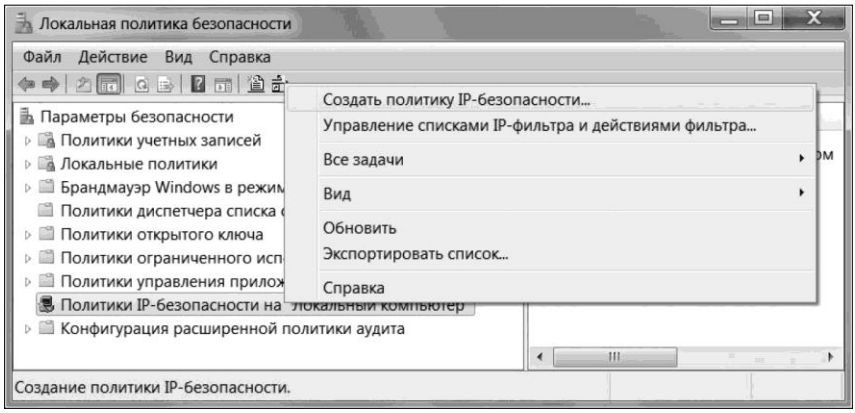
Көліктік режим IP пайдалы деректерін шифрлеу көмегімен екі компьютер арасында қауіпсіз қосылу орнату үшін пайдаланылады. Сондағы IP-тақырыпаты оқуға ғана қол жетімді болып қалады. Authentication Header хаттамасы деректерді мақсатты өзгерістерден қорғайды. Encapsulating Security Payload хаттамасы пайдалы IP деректерінің құпиялығын қамтамасыз етеді, алайда IP тақырыпатын емес.

Туннельдік режим барлық бастапқы IP-пакеттерді шифрлеу қажет болғанда пайдаланылады. Бұл режим қорғалған байланысты ашық байланыс каналдары арқылы деректер жіберуге арналған VPN-туннельдерінің құралдарымен ұйымдастыруға мүмкіндік береді. Authentication Header хаттамасы бүкіл пакетті

шифрлейді, ал бұдан соң оны жаңа пакеттің деректер өрісінде қапшықтайды. Сондағы деректер оқуға қолжетімді болып қала береді. Encapsulating Security Payload хаттамасы бастапқы пакетті ESP тақырыпаты мен ESP шынайылығын тексеру тіркемесі арасына орналастырады да, бір уақытта осы деректерді шифрлеп, жаңа IP тақырыпатын құрады. Туннель сервері каналдың басқа жағында шифрін ашып, алушыға пакетті жібереді.

Windows 7-де IPsec көліктік режимін баптау. Баптау «Жергілікті қауіпсіздіктің саясаты» *(Басқару панелі/Әкімшілендіру/Жергілікті қауіпсіздік саясаты)* жабдығының көмегімен орындалады*:*

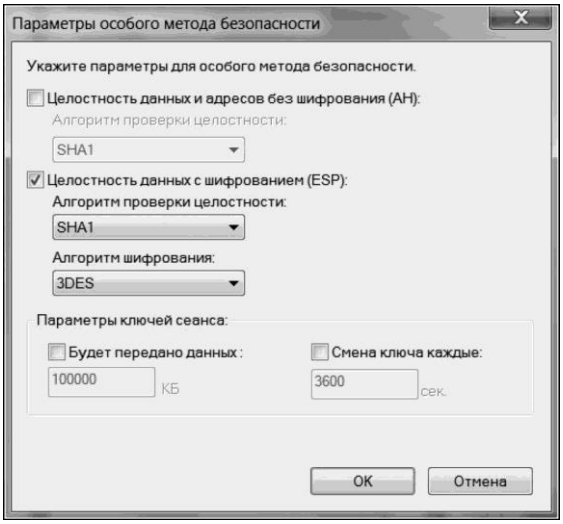
1) IP қауіпсіздік саясатын құру үшін *IP-қауіпсіздік саясаты* тармағын белгілеу және мәнмәтіндік мәзір құралдары арқылы осы элемент үшін IP-қауіпсіздік саясатын құру командасын таңдау (3.15-сурет);
2) Пайда болған *IP-қауіпсіздік саясатының шебері* сұхбат терезесінде *Ары қарай* басу*;*
3) Пайда болған терезеге жаңа саясаттың атын енгізіп, *Ары қарай* басу;
4) Келесі терезеде үнсіз келісім бойынша ережені пайдалану опциясын енгізу;



3.15-сурет. «Жергілікті қауіпсіздік саясаты» жабдығының көмегімен IP қауіпсіздік саясатын құру

5) Шебердің келесі жұмыс қадамында пайдаланушы шынайылығын тексеру тәсілін таңдау:
Kerberos хаттамасы, пайдаланушы сертификаты арқылы немесе кілттермен алмасуды қорғауға арналған жолдардың көмегімен;
6) Қасиеттерді шебер жұмысы аяқталғаннан кейін немесе қажетті саясатты белгілеп, мәнмәтіндік мәзірден *Қасиеттер* тармағын таңдап, кейіннен өзгерту;
7) Қауіпсіздік ережесін құру үшін құрылған IP қауіпсіздік саясатының қасиеттерін ашу, *Шеберді пайдалану* опциясын болдырмау және *Ережелер* қосымшасында *Қосу* батырмасын басу*;*

8) *Қосылу типі* бетбелгісінде құрылатын ереже қандай желелік қосылуларға пайдаланылатынын таңдау;
9) *Шынайылығын тексеру тәсілдері* бетбелгісінде бірнеше тексеру тәсілдерін қосып, оларға артықшылық беру тәртібін өзгерту;
10) Қосылу типі мен шынайылығын тексеру тәсілдерін таңдағаннан кейін IP сүзгісінің тізімін таңдау немесе жаңа сүзгіні құру үшін *IP сүзгілерінің тізімі* қосымшасын пайдалану;
11) Жаңа сүзгіні құру үшін *Қосу* батырмасын басу, бұдан кейін *IP сүзгілерінің тізімі* терезесін ашу, бұнда *Шеберді пайдалану* опциясын болдырмау қажет және сүзгілер тізімінің атын енгізіп, Қосу батырмасын басу*;*
12) Пайда болған *Қасиеттер: IP-Сүзгі* сұхбат терезесінде дереккөзі мен алушының сүзгі, хаттама мен порттары қолданылатын дереккөзінің және пакеттер алушысының мекенжайларын көрсету;
13) *Сүзгі әрекеті* бетбелгісінде сүзгінің әрекетін анықтау*;*
14) Сүзгінің жаңа әрекетін құру үшін *Шеберді қолдану* опциясын болдырмау және *Қосу* батырмасын басу. Ашылған *Қасиеттер: сүзгі әрекетін құру* терезесіндегі *Қауіпсіздік әдістері* қосымшасында деректердің өтуіне рұқсат беру, оларды бұғаттау немесе қауіпсіздігін келісу керек пе екенін көрсету;
15) Егер *Қауіпсіздікті келісу* тармағы таңдалған болса, қауіпсіздік әдістерін қосып, оларға артықшылық беру тәртібін өзгерту. Қауіпсіздік әдістерін қосқан кезде AH, ESP пайдалану керектігін немесе *Бапталатын қауіпсіздік* тармағын таңдап, қауіпсіздікті қолмен баптау керек пе екенін таңдау қажет (осылайша, AH және ESP де іске қосуға болады);
16) *Бапталатын қауіпсіздік* тармағының көмегімен тұтастығы мен шифрленуін тексеру алгоритмін, сонымен қатар сеанс кілттерін ауыстыру параметрлерін таңдау (3.16-сурет).



3.16-сурет. Қауіпсіздік ерекше әдісінің параметрлері

Шифрлейтін файлдық жүйені конфигурациялау. Encrypting File System (EFS) — файл деңгейінде шифрлеуді іске асыратын деректерді шифрлеу жүйесі болып табылатын Windows (Windows 2000 бастап одан да жоғары, үй нұсқасын қоспағанда)құрамдас бөлігі.

EFS құралдарымен деректерді шифрлеу (немесе шифрлеуді болдырмау) үшін файл немесе папка қасиеттерінде тиісті опцияны қосу (өшіру) жеткілікті. Сонымен қатар осы файл немесе папкаға кім қол жеткізу алатынын көрсету мүмкіндігі бар. Осылайша, EFS ақпараттың құпиялығын рұқсат етпей қол жеткізуден қорғау үшін NTFS файлдық операцияларының деңгейінде деректерді шифрлеу, сонымен қатар шифрленген деректерді (Emergency Data Recovery Policy) қалпына келтіру мүмкіндіктерін береді.

EFS файлдарды қорғау мақсатында симметриялы шифрлеуді, сондай-ақ әр файл үшін шифрлеудің кездейсоқ туындаған кілтін қорғау мақсатында ашық/жабық кілт жұбына негізделген шифрлеуді пайдаланады.

Active Directory доменінің құрамына кіретін барлық компьютерлер EFS ұстайды. Active Directory доменіне қосылған компьютерде EFS ұстайтын опцияны бақылап тұру мүмкін емес, себебі бұндай мүмкіндік үнсіз келісім бойынша доменнің саясатымен бақыланады.

Windows 2000 кейін шыққан Windows операциялық жүйесі деректерді шифрлеу үшін деректерді қалпына келтіру агенттерін талап етпейді. EFS топтық саясат объектілеріне деректерді қалпына келтіру агентінің сертификатын қосумен бақыланбайды.

Топтық саясат параметрлерінің көмегімен EFS баптау. Топтық саясат параметрлерін конфигурациялау белгілі бір қауіпсіздік талаптарына сәйкес

доменге кіретін компьютерлерді баптауға мүмкіндік береді.

Шифрленген файлдық жүйені баптау үшін мынадай іс-әрекеттерді орындау қажет:

1) *Топтық саясаттарды басқару редакторы* ашу және *Компьютер конфигурациясы/Саясаттар/ Windows конфигурациясы/Қауіпсіздік параметрлері/Ашық кілт саясаттары/Шифрленген файлдық жүйе* торабын таңдау;
2) Осы торап үшін мәнмәтіндік мәзір құралдары арқылы *Қасиеттер: Шифрленген файлдық жүйе* сұхбат терезесін ашып, *Қасиеттер* командасын таңдау;
3) барлық талап етілетін EFS баптауларын жүргізгеннен кейін ОК батырмасын басу.

Қасиеттер: Шифрленген файлдық жүйе сұхбат терезесінде келесі опцияларды баптауға болады:

- «Шифрленген файлдық жүйе (EFS) көмегімен файлдарды шифрлеу» — EFS жүйесінің көмегімен файлдарды шифрлеу мүмкіндігіне жауап береді. Үнсіз келісім бойынша EFS шифрлеу рұқсат етілген;
- «Пайдаланушының «Құжаттар» папкасының ішіндегісін шифрлеу» — пайдаланушының *Құжаттар* папкасын автоматты түрде шифрлеуге мүмкіндік береді;
- «EFS үшін смарт-карта талап ету» — пайдаланушылар шифрленген файлдарға қол жетімділігін алу мақсатында смарт-карталарды қолдануы үшін EFS арналған бағдарламалық жасақтама сертификаттарын пайдалануға тыйым салады;
- «Смарт-картадан бағаланатын пайдаланушы кілтті құру» — алдыңғысы сияқты пайдаланушыдан шифрленген файлға бірінші рет қол жеткізген кезде (осы сеанста) ғана сим-картаны енгізуді талап етеді;
- «Басқылау файлының шифрлеуін енгізу» — басқылау файлының шифрленуіне жауап береді, себебі оның құрамында EFS қорғауы бар файлдардың шифрленбеген көшірмелері болуы мүмкін;
- «Пайдаланушы кілтті құрған немесе өзгерткен кезде кілтті архивтеу туралы хабарламаларды бейнелеу» — жүйе шифрлеу кілттерін құрған және өзгерткен кезде пайдаланушыға EES кілттеріне архивтеу орындауды ұсынады;
- «Сертификаттау орталығына қол жетпегенде EFS-ке өздігінен аяқтайтын сертификаттар құруға рұқсат беру» —пайдаланушыларға EFS көмегімен файлды бірінші рет шифрлеген кезде сертификаттау орталығына жүгінбеуге мүмкіндік береді, яғни сертификаттау орталығына қол жетімділігі жоқ пайдаланушылар EFS қосыла алмайды. EFS жүйесіне сертификаттау орталығынан сертификатты алуға рұқсат беруі үшін сертификаттау орталығын баптап, өтінімдердің автоматты түрде берілуін қосу қажет.

EFS файлдық жүйесімен байланысқан және топтық саясаттарды басқару редакторында қол жетімді басқа да шифрлеу параметрлері бар:

- *К*омпьютер *конфигурациясы*/ *Саясаттар*/ *Әкімшілік шаблондар*/ *Желі*/

Дербес файлдар торабы, *Дербес файлдардың кэшін шифрлеу* элементі дербес файлдарды шифрлеуге жауап береді;

- *Компьютер конфигурациясы*/*Саясаттар*/*Әкімшілік шаблондар*/*Windows құрамдас бөліктері*/ *Кіру* торабы, *Шифрленген файлдарды индекстеуге рұқсат беру* элементі. Шифрленген файлдар индекстеуін өшіру қауіпсіздік деңгейін арттырады. Себебі шифрленген файлдың ішіндегісін индекс көмегімен анықтауға болады.

RADIUS қызметінің көмегімен сәйкестендіру. RADIUS (Remote Authentication Dial-In User Service — қашықтағы пайдаланушалардың шынайылығын тексеру қызметі) қашықтықтан қол жетімділігін беру қызметтері үшін сәйкестендіру, авторландыру және есептік деректерді жинаудың орталықтандырылған құралы болып табылады.RADIUS хаттамасы желілік шабуылдардан қорғанудың бірқатар механизмдерін иеленеді.

Теңтүпнұсқалылық — субъектінің шынайылығын оның сәйкестендіру деректері бойынша тексеруге мүмкіндік беретін процесс.

Авторландыру — белгілі нысандар немесе сервистердің қол жетімділігіне идентификациялық субъектінің өкілеттігін анықтауға мүмкіндік беретін процесс.

Есептік деректерді жинау деп пайдаланылған ресурстар туралы мәліметтер жинауға мүмкіндік беретін процесті айтады.

Желілік құрылғылар жаднамасының қорлары шектеулі болғандықтан RADIUS хаттамасы пайдаланушыларды сәйкестендіру үшін жиі пайдаланылады. Бұл пайдаланушалрдың көбірек саны туралы ақпаратты сақтауға мүмкіндік береді. Іс жүзінде RADIUS барлық дерлік өндірушілердің желілік құрал-жабдықтарын ұстайды.

Хаттама былайша қызмет атқарады:

1. Клиент қатынау сұранысын жасайды (Access-Request) және оны RADIUS-серверге жолдайды. Сұрау салғанда кем дегенде, пайдаланушының есімі мен паролі (шифр қойылған) болуы қажет. Шифрлеу клиент пен сервердің ортақ құпиясының болуына байланысты жүзеге асырылады.
2. RADIUS-сервер өзінің клиентпен ортақ құпияға иелігін тексереді. Егер құпия ортақ болса, сервер клиенттің шифр қойылмаған есімі мен паролін анықтайды.
3. Есімі мен паролі пайдаланушының деректер қорымен салыстырылады.
4. Егер есімі мен паролінің тексеруі сәтті өтсе, RADIUS- сервер қатынауға рұқсат алғаны туралы хабарламаны (Access-Accept) құрып, оны клиентке жолдайды. Басқаша болған жағдайда ол қатынауға рұқсат жоғы туралы хабарлама (Access-Reject) алады.
5. Клиент идентификатор бойынша серверден келген хабарламаны тексереді және егер де идентификатор сәйкес келсе, клиент сұраудағы сұрау жолында не болғанын салыстыру үшін аутентификатордың жауап жолын кодпен ашады.

Windows RADIUS-те теңтұпнұсқа, авторландыру және деректерді есепке алу саясатын орталықтандырып баптауға мүмкіндік беретін желі саясатының серверінде пайдаланылады.

Windows Server 2008-де желі саясатының сервері мынадай нұсқаларда іске

асырылуы мүмкін (серверді бір рет іске асыру нұсқаларының түрлі үйлесімі болуы мүмкін):

- RADIUS -server. Желі саясатының сервері тұпнұсқалылық, авторландыру және деректерді есепке алу тексерісін орталықтандырып орындайды;
- RADIUS-proxy. Желі саясатының сервері қосуға сұрау салу саясатының баптауына байланысты басқа RADIUS-серверлерге сұрауды қайта жібереді;
- Network Access Protection (NAP) policy server (желіге қол жетімділігін қорғау саясатының сервері). Желі саясатының сервері желіге қол жетімділігін қорғау саясаты мен параметрлерін баптауға мүмкіндік береді.

Желі саясатының серверін баптау. Баптаудың екі нұсқасы болуы мүмкін::

1) *стандарттық:* шебердің көмегімен, желі саясаты серверінің консолімен рұқсат етілген;
2) *кеңейтілген:* желі саясаты серверінің функционалдығын қолмен баптауға мүмкіндік береді. Осы баптау желі саясаты сервері консолінің «Қосымша баптау» элементі көмегімен қол жеткізіледі.

Active Directory доменінде желі саясаты серверін пайдалану. Active Directory доменінде пайдаланылатын желі саясатының сервері Active Directory домендік қызметтеріндегі пайдаланушының есептік деректерін пайдаланушының есептік деректерімен салыстыру арқылы теңтүпнұсқалы процесті жүргізуге мүмкіндік береді.

Active Directory домендік қызметтерінде желі саясатының серверін тіркеу үшін мынаны істеу қажет:

1) желі саясаты серверінің консолін ашу; контекст мәзірінің құралдарымен *«Желі саясаттарының сервері» (жергілікті)* элементі үшін Windows Server 2008-де *Серверді тіркеу* командасын таңдау (домен әкімшісінің құқығы талап етіледі);
2) пайда болған сұхбат терезесінде ОК батырмасын басу.

БАҚЫЛАУ СҰРАҚТАРЫ

1. DHCP деген не? Қандай жағдайларда пайдаланылады?
2. DHCP-клиент DHCP-сервермен қатынасты орнатуға қалай бастамашылық етеді?
3. DHCP-клиент пен DHCP-сервер қандай хабарламалармен алмасады?
4. DHCP-клиентке хабарламалармен алмасу журналы бойынша мекенжай берілгенін қалай ұғуға болады?
5. DHCP-сервер баптауында DNS параметрлері қалай қойылады?
6. subnet-те көрсетілген мекенжайларының ауқымы range-де көрсетілгеннен немен ерекшеленеді?
7. Белгілі желілік интерфейсте DHCP арқылы мекенжай алу процесін қалай іске қосады?
8. DHCP, DNS көмегімен тіркелген IP-мекенжайларды қалай баптауға болады?

9. Домендік зона, ресурстік жазба дегеніміз не?
10. Ресурстік жазба қандай құрамдас бөліктерден тұрады? Ресурстік жазбалардың қандай түрлері жиі кездеседі?
11. Домендік атау неден құралады? Бос жолда берілген резервке қалдырылған домендік атау нені білдіреді?
12. Толық домендік атаудың салыстырмалыдан айырмашылығы неде?
13. Салыстырмалы домендік атауды пайдаланған кезде ресурстік жазбаның іздеуі қалай жүргізіледі?
14. Hint, Slave, Master типті домендік зоналардың айырмашылығы неде?
15. DNS-серверінің BIND журнал файлы қайда орналасқан?
16. Атауларға рұқсатты жөнге келтіру қалай іске асырылады?
17. Атауларға рұқсат беру кітапханасы қалай бапталады (DNS клиент)?
18. Active Directory каталогтар қызметінің құрылымына кіретін негізгі объектілер?
19. Пайдаланушыға Windows Server 2008 жаңа орманын орнатудың қандай нұсқалары ұсынылады?
20. Active Directory әкімшілендіру орталығы көмегімен шешілетін әкімшілік жүргізудің басты міндеттері неде?
21. Каталогтарға қол жеткізудің жеңілдетілген хаттамасы дегенді қалай түсінуге болады (LDAP)?

22. Пайдаланушылар есептік жазбаларының шаблондарын пайдаланудың ыңғайлылығы неде?
23. Домендегі топтар әрекетінің қай салаларын білесіз?
24. Доменнің топтық саясаты дегеніміз не?
25. Топтық саясаттарды пайдалану негіздері неде?
26. Топтық саясаттарды мұралану қалай өтеді?
27. Қауіпсіздік шаблондарын баптаудың қандай тәсілдерін білесіз?
28. Қауіпсіздік шаблондары жабдығының жүйелік қызметін пайдалану ыңғайлылығы неде?
29. IP sec нені білдіреді?
30. ISO/OSI моделінің қай деңгейінде IPsec орналасады және не үшін?
31. IPsec қандай хаттамалар енеді?
32. IPsec жұмысының көліктік және туннельдік режимдерінің айырмашылығы неде?
33. ОС Windows-тегі EFS көмегімен деректер шифрлеуін қалай қосуға болады?
34. EFS шифрлеудің қандай түрін пайдаланады?
35. Шалғайдағы пайдаланушылардың шынайылығын тексеру қызметі қандай мүмкіншіліктер береді (RADIUS)?
36. RADIUS әрекеті принципінің мәні неде?
37. Windows Server 2008-де желі саясатының серверін іске асырудың қандай нұсқаларын білесіз?

4 тарау

ЖЕРГІЛІКТІ ЖӘНЕ ЖАҺАНДЫҚ ЖЕЛІЛЕРГЕ ҚОЛ ЖЕТКІЗУДІ ҰЙЫМДАСТЫРУ

4.1. БАҒДАРЛАУ НЕГІЗГІ ҚАҒИДАТЫ

Бағыттау (routing) — бұл байланыс желілеріндегі ақпарат бағытын анықтау процесі. Көбінесе маршрут арнайы бағдарламалық-аппараттық құралдар-*бағдарлауыштар* арқылы анықталады**.**

Бағдарлау OSI (желілік) моделінің үшінші деңгейінде өтеді.

Бағдарлауыш - белгілі бір ережелерге негізделген желілік сегменттер арасында бағдарлау процесін қамтамасыз ететін OSI анықтамалық үлгісінің үшінші қабатының құрылғысы (немесе компьютер).

Бағдарлау жұмысының логикасы. Бағдарлау екі тапсырманы шешуге арналған: пакеттердің бағытын анықтау; пакетті беру үшін коммутация.

Бағытты анықтау. Бағдарлау алгоритмдері бағытты анықтау үшін пайдаланылады,, олар әртүрлі көрсеткіштер (матрик) негізінде, бағдарлау кестелерін толтырады және қолдайды, ол ақпараттық ағынның қолжетімді бағыттары туралы ақпаратты қамтиды.

Бағдарлау кестесі - тағайындалған мекенжайлар мен интерфейстер арасындағы сәйкестікті сипаттайтын электрондық кесте немесе дерекқор, ол арқылы деректер пакетін келесі бағдарлауышқа жіберу керек.

Бағдарлау кестесі әдетте келесі ақпаратты қамтиды:

- тағайындау не нұсқау желінің немесе түйіннің мекен-жайы, яғни бұл бағыт әдепкі бағыт болып табылады;
- желінің тағайындау маскасы;
- көрсетілген бағдарлауыштың көрсетілген мекен-жайға сәйкес келетін пакетті жіберетін желідегі мекен-жайын көрсететін шлюз;
- интерфейс;
- метрика - таңдаулы бағытты анықтайтын сандық көрсеткіш.

Әдетте, метрика жөнелтушінің қабылдағышқа жіберген хабарламасы арқылы өтетін қашықтық (транзиттік бөліктер саны) деп түсініледі. Кішірек метрика (көрсеткіш), неғұрлым бағыт жақсырақ. Бағдарлауыштар үздік бағдарларды анықтау үшін метрикаларды салыстырады.

Шлюз (gateway) - түрлі хаттамалар арқылы компьютерлік желілерді қосу үшін жасалған аппараттық немесе бағдарламалық бағдарлауыш. Әдепкі шлюз - қол жетімді бағдарлау кестелеріне негізделген нақты бағыты жоқ пакеттер жіберілетін шлюз. Пакеттерді қайта бағыттағанда, шлюздер алушының мекен-жайына емес, алушыны қамтитын мақсатты желі мекен-жайына бағытталған.

Бағдарлау кестесінде нақты бағыт болмаған кезде, пайдаланылатын әдепкі шлюздерді көрсете алады. Бағдарлау кестесі бағыт хаттамалары арқылы орнатылады.

Пакеттер табыстау үшін коммутация. Коммутация алгоритмі келесі қадамдар түрінде ұсынылуы мүмкін:

1. Жеткізу орнында пакетті алушыға жіберу міндеті туындайды.
2. Жіберуші бағдарлауыштың физикалық мекен-жайын (MAC-мекен-жайы) алады.
3. Жіберуші бағдарлауыштың қабылдаған физикалық мекен-жайына пакетті жібереді, алайда қабылдаушы хаттаманың мекен-жайынан.
4. Бағдарлауыш пакеттің тағайындалған хаттаманың мекен-жайын тексереді және осы пакетті келесі бағдарлауышқа тасымалдау туралы ақпарат бар-жоғын анықтайды.
5. Егер ақпарат табылса, бағдарлауыш келесі бағдарлауыштың физикалық мекен-жайы арқылы тағайындалған мекенжайдың физикалық мекенжайын ауыстырып, келесі бағдарлауышқа жібереді. Егер ақпарат табылмаса, онда пакет ескерілмейді.
6. 4-5-тармақтар пакет алушыға жеткенше қайталанады, немесе жіберілу кейбір сатысында еленбейді.
7. **Статистикалық және динамикалық бағдарлау.** Бағыттарды екі түрге бөлуге болады: статикалық, әкімшілікті түрде белгіленетін; динамикалық, бағдарлау алгоритмдерін пайдалану арқылы есептелетін, бағдарлау хаттамалары арқылы алынған топология және желі күйі туралы ақпаратқа негізделген.

Статикалық бағыттау әкімшімен бағдарлауыш реттеу кезінде бағытты қолмен қосуын қарастырады.

Статикалық бағдарлаудың баптау міндеті шағын желілерде оңай шешіледі. Бұл бағдарлауыштың тағы бір артықшылығы - желіге қосымша жүктеме болмауы, себебі динамикалық баптау құралдары пайдаланылмайды.

Статикалық бағдарлаудың кемшіліктері масштабтаудың күрделілігіне (бағытты реттеу үшін әкімшінің қатысуын талап етеді) және желі ақауларын бақылайтын қиындықтар.

Динамикалық бағдарлау, бағдарлау кестелерін бағдарламалық жасақтаманы өңдеуді қамтиды. Бағдарлау кестелерін өңдеуге арналған бағдарламалық қамтамасыз ету, кестелерді пакеттерге арналған оңтайлы бағытпен толтыру үшін қажет, өзара ақпарат алмасады. Бағдарлау кестелерді динамикалық толтыру үшін қажетті ақпарат алмасу динамикалық бағдарлау хаттамаларын қолдану арқылы жүзеге асырылады. Мұндай ақпарат, мысалы, метрика немесе кейбір басқа көрсеткіштер немесе олардың тіркесімі болуы мүмкін.

Бағдарлау бағдарламалық құралы екі режимнің бірінде жұмыс істей алады:

- **белсенді,** бағдарлау туралы ақпаратты мерзімді жіберуді және басқа хосттар мен шлюздерден ұқсас хабарламаларды алуды қамтамасыз етеді;
- **пассивті,** Ол бағдарлау туралы ақпарат алуды ғана шамаланған.

Бағдарлау хаттамалары- бағдарлау кестелерін автоматты түрде толтыруға арналған арнайы хаттамаларБағдарлау хаттамалары бағдарлау кестелерін толтыру тәсілімен ерекшеленеді, оңтайлы бағытты таңдау өлшемі және басқа да мүмкіндіктерді көрсету жолымен ерекшеленеді.

Бағдарлау хаттамалары әртүрлі бағдарлау алгоритмдері арқылы іске асырылуы мүмкін**.**

Бағдарлау алгоритмдері келесі сипаттамаларға сәйкес жіктелуі мүмкін.

1. *Оңтайлы бағытты таңдау әдісін қолдану:*

- бір сатылы, онда пакеттің әр өту кезеңінде, бағдарлауыш тек келесі бекетке жіберу үшін жауап береді;
- көп сатылы, оның құрамында барлық тасымалдау транзиті бағдарлауыштарды қоса алғанда, пакет бастапқыдан толық бағыты бар, жөнелту түйіннен бастап белгіленген пунктке дейін. Осы тәсілмен бағдарлау кестелерін талдаудың қажеті жоқ, бұл пакетті беру жылдамдығын арттырады, бірақ бастапқы түйіндердің қосымша жүктемесі бар.

2. *Бағдарлау кестелерін құру әдісі арқылы:*

- статикалық бағдарлау алгоритмдері, әдетте, желі әкімшісімен қолмен бапталады;
- бағдарлау кестелерін пайдаланбай қарапайым бағдарлау алгоритмдері. Қарапайым бағдарлаудың төрт түрі бар:

а Кездейсоқ бағдарлау - бағдарлауышпен алған пакет кездейсоқ бағытқа жіберіледі; а көшкінді бағдарлау - жіберілім тарату ауқымы кең барлық қолжетімді бағыттарға жіберіледі; а ең қысқа кезек - пакет ең аз жүктелген портқа жіберіледі;

бағдарлау жинақталған тәжірибені ескере отырып - түсетін пакеттер мекенжайы белгіленген кестесі қолданылады;

- бағдарлау кестелерін автоматты түрде толтыратын динамикалық бағдарлау алгоритмдері. Бұл алгоритмдер бейімделгіш деп те аталады, себебі олар желілік топологияны өзгерткен кезде ағдарлау кестелерін автоматты түрде баптайды.

3. *Бағдарлауыштармен алмасқан ақпарат түрі бойынша*:

- RIP(Routing Information Protocol — ақпаратты бағыттау хаттамасы) хаттамаларында пайдаланылатын қашық-векторлық алгоритмдер, IGRP (Interior Gateway Routing Protocol), BGP (Border GateWay Protocol — шекаралық шлюз хаттамасы), AODV (Ad hoc On-Demand Distance Vector). Бағдарлауыштар уақытша көршілес тораптарға белгілі ішкі желілер туралы ақпаратты және оларға дейінгі қашықтықты (транзиттік тораптар саны) жібереді;
- IS-IS (Intermediate System to Intermediate System — ішкі хаттама шлюздері) хаттамаларында пайдаланылатын байланыс жағдайының алгоритмдері, OSPF (Open Shortest Path First — ең қысқа бағыттын ашық хаттамасы), NLSP (Netware Link Services Protocol) және басқа. Әр бағдарлауыш желінің нақты топологиясын құру үшін қажетті ақпаратпен қамтамасыз етіледі, көршілес түйіндер және ішкі желілер

ақпарат алмасу туралы.

Статикалық және динамикалық бағдарлауды баптау.

Жоғарыда айтылғандай, статикалық бағдарлау, бағдарлау кестелерін желілік әкімші тарапынан қолмен реттеуін қамтиды. Төменде Windows Server 2008 бағдарламасында статикалық бағдарлаудың баптау мысалы келтірілген.

Windows Server 2008 нұсқасында, Windows жүйесінің бұрынғы нұсқаларында көрсетілгендей, статикалық бағдарлауды баптаудың екі тәсілі бар: пайдаланушы графикалық интерфейсі арқылы; пәрмендік жолды пайдаланып, route пәрмені арқылы.

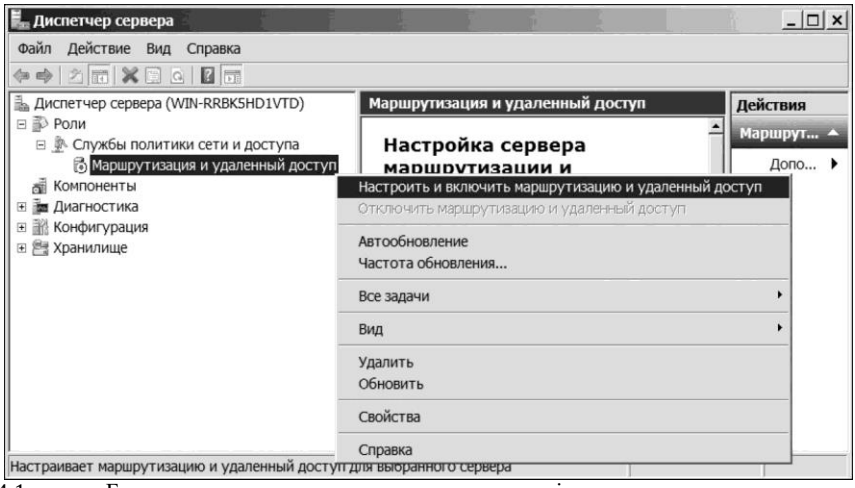
Пайдаланушы интерфейсі арқылы бағыттарды жасау. Бағыттын баптауын бастамас бұрын, бағдарламалық бағдарлауыш болып табылатын және Windows Server 2008 жүйесіндегі IPv4 және IPv6 желілерінде бағдарлауды қамтамасыз ететін Бағдарлау және қашықтан қатынау қызметін (RRAS) орнату қажет.

Бағдарлау және қашықтан қатынасу қызметін орнату үшін келесі әрекеттерді орындауыңыз керек:

1) рөлді қосу үшін, Бастау мәзірін пайдаланып «Сервер диспетчері» қосымшасын іске қосу қажет **Әкімшіліктендіру / Сервер диспетчері және Рөлдер мәнмәтіндік мәзірінде Рөлдерді қосу түймешігін басыңыз;**
2) **Рөлдерді қосу шебері тілқатысу терезесінде Жұмысты бастамас бұрын бетінде Келесі түймешігін басыңыз;**
3) Сервер ролдері *бетінде Желі және қатынас саясаты қызметтері* тармағын таңдап, *Келесі* түймешігін басыңыз.;
4) Рөлдік қызметтер бетінде Бағдарлау және қашықтан қатынасу қызметтерін таңдаңыз;
5) *Растау* бетінде *Орнату* түймешігін басыңыз, орнатудан кейін орнату нәтижелерін оқып, *Жабу* түймешігін басыңыз..

Бағдарлау рөлі мен қашықтан қатынасу қосқаннан кейін, осы қызметті жергілікті және жаһандық желі бағдарлауыш ретінде қосу керек:

1) Бағдарлау және қашықтан қатынасу қызмет консолін ашыңыз. *Бастау* мәзірінен *Әкімшіліктендіру / Сервер диспетчері* арқылы сервер рөлдерін бөлімін ашыңыз және *Желілік саясат және кіру қызметтері / Бағдарлау және қашықтан қатынасу* тармағын таңдаңыз;



4.1. сурет. Бағдарлау және қашықтан қатынасу қызметін қосу

2) *Бағдарлау және қашықтан қатынасу түйініне арналған мәнмәтіндік мәзірді пайдалану арқылы Бағдарлау және қашықтан қатынасуды реттеу және қосу пәрменін таңдаңыз (4.1-сурет);*

3) *Бағдарлау серверін және қашықтан қатынасуды* орнату шеберінің сәлемдесу терезесінде *Келесі* түймешігін басыңыз және *Конфигурация* шеберінің келесі бетінде *Ерекше конфигурация* пәрменін таңдап, *Келесі* түймесін басыңыз (4.2-сурет);

4) шебердің келесі бетінде серверде іске қосылатын қызметтерді көрсетіңіз. Жергілікті желіні бағдарлау опциясын таңдап, *Келесі* түймесін басыңыз.**;**

5) шебер жұмысының аяқтау кезеңінде Дайын түймешігін басыңыз..

Бағдарлау және қашықтан қатынасу қызметтерін мәнмәтіндік мәзір құралдары арқылы сипаттар тілқатысу терезесін шақырып *Бағдарлау және қашықтан қатынасу қызметін* баптауға болады**.**

Тұрақты IPv4 маршрутын жасау үшін келесі әрекеттерді орындауыңыз керек:

1) Бағдарлау және қашықтан қатынасу қызмет консолін ашыңыз(Желілік саясат және кіру қызметтері/Бағдарлау және қашықтан қатынасу серверінің диспетчері элементі);

2) IPv4 түйінін кеңейтіңіз IPv4 түйінінде / статикалық бағыттар мәтінмәндік мәзірін пайдаланып, Жаңа статикалық бағыт пәрменін таңдаңыз (4.3-сурет);

пайда болған тілқатысу терезесінде IPv4 Статикалық бағыты келесі өрістермен толтырады (немесе қол жетімді нұсқалардан таңдаңыз):

■ **Интерфейс - желіге пакеттерді жіберу үшін пайдаланылатын интерфейсті таңдауға мүмкіндік береді**;

Бағдарлау және қашықтан қатынасу серверін баптау шебері

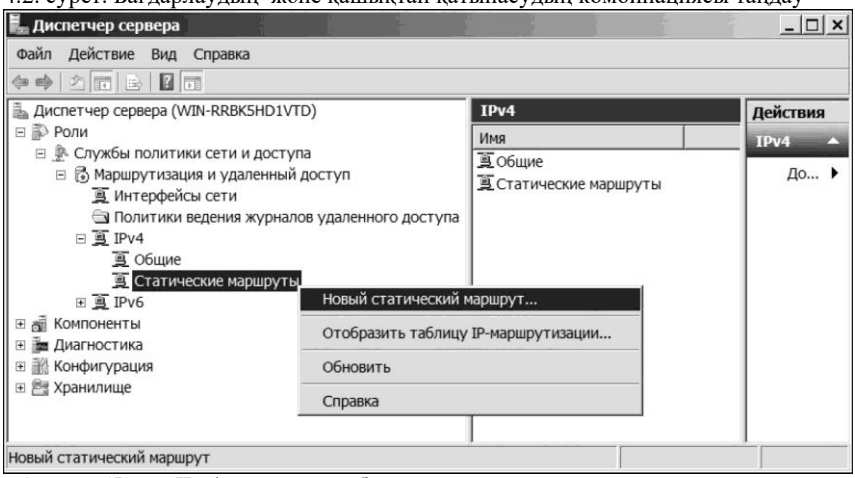
Конфигур а ция
Көрсетілген қызметтерді осы үйлестірудің кез-келгенінде қосуға немесе осы серверді теңшеуге болады.

С Қашықтан қатынасу (VPN немесе модем)
Қашықтағы клиенттерге осы серверге қашықтағы байланыс арқылы қосылу немесе виртуалды жеке желіге (VPN) қауіпсіз қосылуды қамтамасыз етеді.
С Желілік мекен-жайларды түрлендіру (NAT)
Ішкі клиенттерге жалпы IP мекенжайын пайдаланып Интернетке қосылу мүмкіндігін береді.
С Виртуалды жеке желіге (VPN) және NAT-ға қолжетімділік
Қашықтағы клиенттерге және ішкі клиенттерге осы серверге бір жалпы IP мекенжайын пайдаланып Интернетке қосылу үшін мүмкіндік береді.
С Екі жеке желі арасында қауіпсіз байланыс
Бұл желіні қашықтағы желіге, мысалы, филиал желісіне қосуға мүмкіндік береді.
Ц Ерекше конфигурациясы
Бағдарлаудың және қашықтан қатынасу мүмкіндіктерінің кез келген комбинациясы.

Толығырақ

«Артқа I Әрі> I Жою

4.2. сурет. Бағдарлаудың және қашықтан қатынасудың комбинациясы таңдау



4.3.сурет. Жаңа IPv4 статикалық бағытты жасау

■ ***Тағайындау — IPv4- желі мекен-жайына жауап береді***;

- ***Ішкі желі маскасы — желілік мекен жайға сәйкес маска енгізу үшін пайдаланылады***;
- ***Шлюз- онда транзиттік түйін ретінде пайдаланылатын бағдарлауыштың IPv4-мекенжайын енгізу керек***;
- ***Метрика — бағытты жүріп өту шығындарын көрсетеді***;

3) жаңа IPv4 бағытын орнатуды аяқтағаннан кейін ОК түймешігін басыңыз.

IPv6 статикалық бағытты жасау үшін келесі әрекеттерді орындау қажет::

1) Бағдарлау және қашықтан қатынасу қызмет консолін ашыңыз;
2) IPv6 түйінін кеңейтіңіз және мәтінмәндік мәзірі арқылы IPv6 түйінінде / Статикалық бағыттар Жаңа статикалық бағыт пәрменін таңдаңыз***;***
3) IPv6 Статикалық бағыт пайда болған тілқатысу терезесінде келесі өрістерді толтырыңыз:

- ***Интерфейс*** — желіге пакеттерді жіберу үшін пайдаланылатын интерфейсті таңдауға мүмкіндік береді;
- ***Тағайындау - желінің IPv6 мекен-жайы үшін жауапты (екі нүктелі оналтылық түрге дейін);***
- ***Префикстің ұзындығы — тағайындау мекенжайдағы желілік мекенжайды білдіретін биттердің санына жауап береді***;
- ***Шлюз*** — транзитті түйін ретінде пайдаланылатын бағдарлауыштың IPv6 мекенжайын енгізу керек;
- ***Метрика — бағытты жүріп өту шығындарын көрсетеді***;

4) жаңа IPv6 бағытын орнатуды аяқтағаннан кейін ОК түймешігін басыңыз.

Route пәрмені арқылы бағыттарды құру. Бағдарлау кестесін көру үшін, route print пәрменді пайдалануыңыз қажет**.**

Interface list (интерфейс тізімі) Windows Server IP интерфейстерінің нөмірлері бар. Содан кейін IPv4 Route Table (IPv4 бағдарлау кестесі) және IPv6 Route Table (IPv6 бағдарлау кестесі) жүреді.

Статикалық бағытты қосу ***route add*** пәрменді қолдану арқылы жүзеге асырылады**.** Мысалы:

route add 10.10.10.0 mask 255.255.255.0 10.10.1.1 if 1

Бағытты қосқанда, сіз осы маршрут үшін желі мекенжайын, масканы, шлюзді, метриканы және интерфейсті көрсетесіз.

Статикалық бағытты жою үшін ***route delete*** пәрменді пайдаланыңыз**.** Бұл ретте тек желі мекенжайы ***route delete*** көрсетіледі
10.10.10.0.

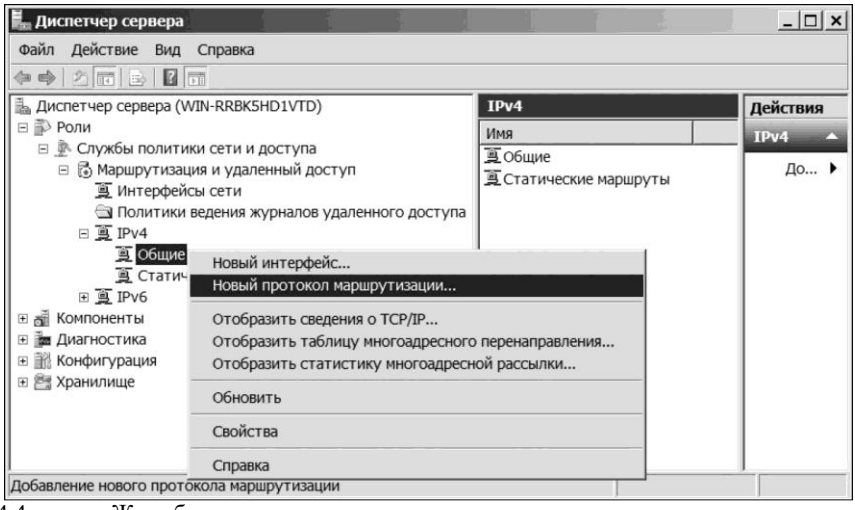
Windows Server 2008 жүйесінде динамикалық бағдарлауды баптау. Динамикалық бағдарлау баптауы, статикалық бағдарлау баптауына ұқсас, бағдарлау және қашықтан қатынасу қызметтерін орнатудан және оны іске қосудан басталады.

Бұдан әрі кіші және орта желілерде бағдарлау туралы ақпаратпен алмасу үшін бағытты ақпараттық хаттамасын (RIP) қосу қарастырылады.

Бағдарлау хаттамасын қосу үшін келесі әрекеттерді орындауыңыз керек:

1) Бағдарлау және қашықтан қатынасу қызмет консолін ашыңыз (Желілік саясат және кіру қызметтері / Бағдарлау және қашықтан қатынасу сервер диспетчерінің элементі);
2) IPv4 торабын кеңейтіңіз және IPv4 / Жалпы тораптағы мәтінмәндік мәзірі арқылы, *Жаңа бағдарлау хаттамасының* пәрменін таңдаңыз (4.4-сурет);в пайда болған *Жаңа бағдарлау хаттамасының* тілқатысу терезесінде IP үшін RIP 2 нұсқасын таңдап, *OK* түймесін басыңыз.

Бағдарлау ақпараттық хаттамасын баптау келесі әрекеттерді қамтамасыз етеді:



4.4. сурет. Жаңа бағдарлау хаттамасын қосу

1) *Жаңа интерфейс* пәрменін таңдау үшін RIP түйінінің мәтінмәндік мәзірін пайдаланыңыз және *Local Area Connection* тармағын таңдап, OK түймесін басыңыз; Пайда *болған RIP - Local Area Connection* тілқатысу терезесінде орындалатын тапсырмаға байланысты қосымша интерфейсті теңшеңіз..

RIP хаттамасының интерфейстерінің қасиеттері туралы қосымша ақпарат алу үшін ресми Microsoft TechNet веб-сайтына кіріңіз.

4.2. СЫМСЫЗ БАЙЛАНЫС ЖЕЛІЛЕРІНЕ ҚОЛ ЖЕТКІЗУДІ ҰЙЫМДАСТЫРУ

Wi-Fi рұқсат нүктесі — Бұл сымсыз желі жасау үшін немесе бар сымсыз желіге кіру үшін пайдаланылатын желі құрылғысы. Бұл құрылғылар IEEE 802.11 стандарттарында негізделген. Әдетте Wi-Fi рұқсат нүктелері ұялы желіге немесе шеткері құрылғыға қол жеткізуді қамтамасыз ету үшін пайдаланылады. Сымсыз желі коммутатор ретінде Wi-Fi рұқсат нүктесін пайдаланады, Infrastructure режимінде жұмыс істейді, ол екі жолдың бірінде жұмыс істей алады:

Basic Service Set - негізгі режим, ол бір рұқсат нүктесін пайдалануын білдіреді;

Extended Service Set — кеңейтілген режим бірнеше желілер біріктіру үшін, негізгі режимде жұмыс істейді.

1) Рұқсат нүктесін пайдаланып, сымсыз желіні қолдану үшін, төмендегілерді орындауыңыз керек:
2) Рұқсат нүктесінің IP-мекен-жайын, сондай-ақ оның реттеуіне қол жеткізу үшін құпиясөзді анықтаңыз. Бұл ақпаратты рұқсат нүктесінің құжаттамасынан табуға болады немесе егер сіз оны теңшеген болсаңыз, желі әкімшісімен байланыса аласыз. Мысалы Wi-Fi рұқсат нүктесінің IP мекенжайы 192.168.1.100;
3) сымсыз желіге кіруге тиісті компьютерлерді баптау қажет. Олардың IP мекенжайлары рұқсат нүктесі бар сол ішкі желіден болуы керек. Компьютердің IP-мекен-жайын баптау үшін, Басқару тақтасы / Желі және Интернет / Желі қосылымдары к директориясында желі байланысының сипаттарын ашыңыз;
4) Желіге қосылу сипаттары диалогтық терезесінде Интернет хаттамасының нұсқасын (TCP / IPv4) таңдап, Сипаттар түймешігін басу керек;
5) Internet Protocol 4-нұсқасы (TCP / IPv4) Сипаттар диалогтық терезесінде IP мекенжайын және Ішкі желі маскасы өрістерін толтырыңыз, содан кейін OK түймешігін басыңыз;
6) Wi-Fi рұқсат нүктесін баптау керек. Ол үшін браузердің мекенжай жолында рұқсат нүктесінің IP-мекен-жайын енгізіңіз және «Қосу» басыңыз;
7) пайда болатын тілқатысу терезесінде рұқсат нүктесінің баптауын қатынасатын әкімшінің тіркелгі деректерін енгізіңіз (пайдаланушы аты мен құпиясөз құрылғының құжаттамасынан таба аласыз);
8) рұқсат нүктесінің реттеуіне қол жеткізген соң, барлық сипаттар жиынын өзгертуге

болады, соның ішінде:

- Рұқсат нүктесінің IP мекенжайы;
- сымсыз желі атауы (SSID);
- пайдаланылған хаттама;
- режимі (бірнеше хаттамалар болған жағдайда, режим араласады);
- арна ені;
- арна;
- деректерді берудің ең жоғары жылдамдығы.

Параметрлер жиынтығы, сондай-ақ олардың атаулары мен мәндері әртүрлі өндірушілер мен модель құрылғыларына әртүрлі болуы мүмкін. Дегенмен, жабдыққа арналған құжаттамада баптау туралы толық ақпарат бар. Рұқсат нүктелерін баптау, құрылғыларды өндірушілер ұсынған шеберлер арқылы жүзеге асырылуы мүмкін екендігін атап өткен жөн. Пайдаланушы шақыруы (жылдам реттеу деп аталады) құрылғы реттеуіне алғаш кірген кезде автоматты түрде іске қосылады. Егер шебер автоматты түрде іске қосылмаса, браузер арқылы немесе құрылғымен бірге жеткізілетін бағдарламалық құрал арқылы қол жетімді болатын рұқсат нүктесінің интерфейс мәзіріндегі «жылдам орнату» пунктін табу қажет.

4.3. ПРОКСИ - СЕРВЕРДІҢ КЭШТЕУІН ҰЙЫМДАСТЫРУ

Кэштеу прокси-серверін ұйымдастыру Squid мысалын қолданып, ашық және дәлелденген прокси-сервері арқылы тексерілетін болады.. Squid барлық UNIX / Linux жүйелерінде, сондай-ақ Windows 2000 нұсқасынан бастап Windows 2000 жүйесінде жұмыс істей алады.

Windows үшін Squid орнату үшін орнатушы жоқ және оның баптауы мәтіндік файл конфигурациясы редакциялау құралдарымен арқылы жасалады (* .conf).

Squid прокси серверін орнату және іске қосу үшін келесі әрекеттерді орындауыңыз керек:

1) Squid дистрибутивін ашыңыз (C: / Squid / директориясы Squid конфигурация файлдарында әдепкі бойынша көрсетіледі);
2) конфигурация файлдарын жасау. Дистрибутив бумасы ашылғаннан кейін, конфигурация файлының үлгілері C: / Squid / etc / папкасында орналасқан. Файлдардың әрқайсысының мазмұнын жаңа мәтіндік файлға көшіріп, оларды сақтау керек. Жасалған конфигурация файлдарының атаулары үлгі үлгілерімен бірдей болуы керек, бірақ .default кеңейтуін қоспай. Мысалы, squid. conf. default файлының мазмұнын squid. conf деп аталатын файлға көшірілуі керек. conf және сақтау керек;
3) squid. conf. файлын баптаңыз. Егер дистрибутив C: / Squid / өзгеше директориядан ашылса, файлдағы дистрибутив жолын өзгерту керек, «#» белгісін өзгертілген параметрлерден бұрын жою қажет:

- Кэшті сақтауға жауапты *cache_dir* параметрі үшін мәнді көрсетуіңіз керек:

cache dir ufs "Путь к Squid"/squid/var/cache 100 16 256

Веб-сұраулардың лог-файлын сақтауға жауап беретін *access_log* параметрі үшін:

access log c:/squid/var/logs/access. log squid

- прокси сервердің жұмысы туралы ақпаратты сақтауға жауап беретін *cache_log* параметрі үшін:

cache log "Путь к Squid"/squid/var/logs/cache.log

cache_store_log параметрі үшін (кэштегі нысандардың әрекетін көрсететін storage manager үшін лог файлының жолы):

cache store log "Путь к Squid"/squid/var/logs/store. log

- Басқа файлдарға арналған жолды бірдей жолмен өзгерту қажет болуы мүмкін;

4) мына пәрменді пайдаланып, кэшті сақтау үшін папкаларды жасаңыз ***C:/ squid/sbin/squid —z,*** оны пәрмен жолында іске қосу қажет;
5) Squid қызметін орнату мынапәрмен көмегімен ***C:/squid/sbin/ squid —i, ,*** оны пәрмен жолында іске қосу қажет. Осы пәрменді іске қосқаннан кейін Squid прокси сервері қызметі Windows іске қосылғанда іске қосылады;
6) Squid қызметін пәрмен арқылы іске қосу ***C:/net start squid,*** оны пәрмен жолында іске қосу қажет.

Access Control List-ті баптау. Access Control List (ACL) — қатынауды бақылау тізімдері. ACL көмегімен Squid қызметі клиенттің сұрауларының белгіленген ережелеріне сәйкестігін тексереді. Осылайша, ACL әрбір сұрау үшін жеке ереже жасауға мүмкіндік береді. ACL-дің, әр алуан мақсаттарда қолданылатын көптеген түрлері бар, алайда ACL-дің ең көп тараған қолданылысы – сыртқы клиенттерден қосылуларды бұғаттау.

Сұрау алынған кезде Squid ACL-ті тексереді. Өтініш ACL-де сипатталған ережелерге сәйкес бірқатар сынақтардан өтеді:

- рұқсат беру ережелеріне сұрауды тексеру **(*Allow*);**
- тыйым салу ережелеріне сұрауды тексеру **(*Deny*);**
- `Барлығына рұқсат беру` (`Allow all`) немесе `Барлығына тыйым салу` (`Deny all`) *ережелерінің бар-жоқтығын тексеру*.

squid.conf конфигурация файлында Squid прокси-серверінің негізгі баптауларына жауап беретін параметрлер сақталады.

http_port параметрі прокси-сервердің мекен-жайы мен портына жауап береді. Егер прокси-сервер 192.168.0.100 IP-мекенжайы бар компьютерде 3128 порты арқылы қосулы болса, онда ***http_port*** параметрі келесі мағынамен белгіленуі тиіс:

http port 192.168.0.100:3128.

http_access параметрі, ACL-да белгіленген белгілі бір желілік объектілерге қатынауды рұқсат етуге немесе тыйым салуға қолданылады:

ACL жолақтарын қосу үшін келесі қалыптар қолданылады:

acl <аты> <элемент> <тізім > http access <нұсқау> <аты>

<элемент> параметрі ретінде келесілер қолданылуы мүмкін:

- ***src*** — прокси-серверге сұрау келген көздің IP-мекенжайы көрсетіліп жатқанын білдіреді;
- ***dst*** — прокси-сервер клиенті сұрау жіберу әрекетін жасап жатқан тағайындалу IP-мекенжайы көрсетіліп тұрғандығын білдіреді;
- ***srcdomain*** — прокси-серверге сұрау жасалатын домен көрсетілгенін білдіреді;
- ***dstdomain*** — прокси-сервер клиенті сұрау жіберу әрекетін жасап жатқан домен көрсетіліп тұрғандығын білдіреді;
- ***port*** — прокси-сервер клиенті тұрақты өрнектерді қолдану арқылы сұрау жіберу әрекетін жасап жатқан тағайындалу портының нөмірі көрсетіліп тұрғандығын білдіреді;
- ***proto*** — сұрауды тапсыру протоколы белгіленетінін білдіреді;
- [— i] ***srcdom_regex*** — прокси серверіне сұрау әдеттегі өрнектерді пайдаланып келген домен көрсетілетінін білдіреді. *i* кілті тұрақты өрнектердегі символдар регистрын елемеу қажет болған жайдайда қолданылады;
- [— i] ***dstdom_regex*** — прокси-сервер клиенті тұрақты өрнектерді қолдану арқылы сұрау жіберу әрекетін жасап жатқан домен көрсетіліп тұрғандығын білдіреді;
- [— i] ***url_regex*** — URL үшін тұрақты өрнек үлгісі көрсетілгенін білдіреді;
- ***time <күн/күндер>*** <бастапқы уақыт—қорытынды уақыт > — клиенттерді қатынау уақыты бойынша шектеу. Күндер келесі мағыналарға ие болуы мүмкін: ***M*** — дүйсенбі, ***T*** — сейсенбі, ***W*** — сәрсенбі, ***H*** — бейсенбі, ***F*** — жұма, А — сенбі, ***S*** — жексенбі. «Бастапқы уақыт» параметрі «Қорытынды уақыт» параметрінен аз болуы тиіс. ACL ережелерінің қолданылу мысалдары:
- 192.168.1.13 мекенжайы бар клиенттен басқа барлық клиенттерге прокси-серверге кіруге рұқсат беру:

```
acl BlackList src 192.168.1.13 http access deny BlackList
http access allow all
```

- BlackList клиентіне 192.168.0.0/16 ішкі желісіне қатынауға тыйым салу:

```
acl BlackNet dst 192.168.0.0/16 http access deny
BlackList BlackNet
```

- BlackList клиентіне example.com сайтына кіруге тыйым салу:

```
acl BlackSite dstdomain . example. com http access deny
BlackList BlackSite
```

- BlackList клиентіне *.com* аймағындағы сайттарға кіруіне тыйым салу:

```
Acl BlackSites dstdom regex \. com$ http access deny
BlackList BlackSites
```

■ Прокси серверінің барлық клиенттеріне 9000-9099 нөмірлі порттар арқылы жұмыс істейтін бағдарламаларды пайдалануға тыйым салу:

acl BlackPort port 9000-9099 http access deny all
BlackPort

■ FTP протоколын тек BlackList клиенті үшін пайдалануға рұқсат ету:

acl BlackFTP proto ftp
http access allow BlackList BlackFTP
http access deny all

■ демалыс күндері 13.00-ден 14.00-ге дейін BlackList клиентінің прокси-серверге кіруіне тыйым салу:

acl BlackTime time AS 13:00-14:00 http access deny BlackList BlackTime

Пайдаланушылардың түпнұсқаландыруын пайдалану. Squid прокси-серверінде түпнұсқаландырудың тәсімдерін баптау үшін **auth_param** негізгі сөзі қолданылады.

Түпнұсқаландыру тәсімдері үшін ережелерді жазу форматы келесідей:

auth param <тәсім> <параметр> [опциялар]

Түпнұсқаландыру тәсімдері клиентке конфигурациялық файлдағы ену тәртібіне сай көрсетіледі. Тәсімдердің өзгертілуі кезінде Squid прокси-серверлерін қайта қосу қажет етіледі.

Squid-де браузер арқылы клиенттің прокси-серверіне қатынау барысында аутентификация процесін бастауға болады, осындай жағдайда пайдаланушының тіркелгі деректері сұралады. Дұрыс емес деректерді немесе прокси-серверге қатынай алмайтын пайдаланушының деректерін енгізу кезінде, кіруге тыйым салынады. Түпнұсқаландыруды пайдалану үшін, клиент атына негізделген ережені қосу қажет, осы кезде қосылып жатқан ACL жолағы **%LOGIN айнымалы шамасы бар, proxy_auth, proxy_auth_regex** немесе **external** кілттерін қолдануы тиіс.

Squid-та түпнұсқаландырудың келесі тәсімдері қолданылады:

■ **Basic** — негізгі тәсім;
■ **Digest** —H(A1) хэштерін қолдану арқылы;
■ **NTLM** —NTLMSSP протоколын пайдалану арқылы;
■ **Negotiate** —SPNEGO протоколын пайдалану арқылы.

Түпнұсқаландырудың негізгі сұлбасын толығырақ қарастырайық.

Бұл схемада сыртқы түпнұсқаландыру бағдарламасы пайдаланылады және бағдарлама пайдаланушы аты мен құпия сөзі бар жолды оқуы керек. Тіркелгі деректерін енгізген жағдайда сыртқы түпнұсқаландыру бағдарламасы прокси-серверге енгізілген деректердің дұрыстығына байланысты жауап беруі керек. Бағдарламаны белгілеу үшін келесі жол пайдаланылады:

auth param basic program <сыртқы түпнұсқаландыру бағдарламасына жол > <клиенттердің есептік деректері бар файлға жол >

Келесі баптаулар қолданылуы мүмкін:

■ **children** — бір мезгілде іске қосылуы мүмкін түпнұсқаландыру бағдарламасының процестерінің саны:

auth param basic children 10

■ **concurrency** — түпнұсқаландыру үшін бір мезгілде мүмкін болатын сұраулар / арналар саны:

auth param basic concurrency 5

■ **realm** — кіру терезесінде пайдаланушыға жіберілетін жолды анықтайды:

auth param basic realm Squid proxy

■ **credentialsttl** — Squid қаншалықты көп уақыт бойы пайдаланушылардың есептік деректерін (аты мен құпиясөзі) кэштейтінін көрсетеді. Бұл уақыттың аяқталуынан кейін Squid қайтадан пайдаланушының теңнұсқаландыруын сұрайды.

auth param basic credentialsttl 1 hours

■ **casesensitive** — пайдаланушылардың аттарының регистрға сезімталдығын анықтайды:

auth param basic casesensitive off

■ **blankpassword** — бос құпиясөздерді қолдауды не қолдамауды анықтайды:

auth param basic blankpassword off

Прокси-серверлердің иерархиясын қолданудың ерекшелігі. Прокси-серверлерді қосудың иерархиялық құрылымы, бір прокси-сервер басқа бірқатар прокси-серверлер үшін ата-аналық болса, желінің белгілі бір сегментінен трафикті азайту үшін пайдаланылуы мүмкін. Сондай-ақ, прокси серверлер тобы жауаптарды сақтауға арналған қосымша кэштерге қызмет етуі мүмкін. Прокси-серверлердің мұндай құрылымдық ұйымдастырылуының әр түрлі қолданулары бар.

Squid прокси-серверінде иерархиялар байланыстың екі түрі негізінде құрастырылады: «ата-анамен» байланыс және «көршімен» байланыс. Осы байланыстарды қолданып, кез-келген күрделі иерархияларды құрастыруға болады.

Прокси-серверлерін иерархиялық құрылымға біріктіру үшін cache_peer директивасы қолданылады:

cache peer <хост> <тип> <http-порт> <icp-порт> [опции]

Жаңа ата-аналық прокси-серверді орнату үшін <түр> параметрінде *parent* мағынасы белгіленеді. Мысалы, егер ағымдағы (бапталып жатқан) прокси-серверге **parent. com хост аты бар ата-аналық прокси-серверді қосу қажет болса,** онда

прокси-сервердің **squid. conf конфигурациялық файлына келесі жолдарды енгізіңіз:**

cache peer parent. com parent 3128 0 no-query default never direct allow all

Екінші жол серверге тікелей қосылуға мүмкіндік бермейді. Алайда, егер ата-аналық прокси сервері қандай да бір себептермен қол жетімді болмаса, ағымдағы серверге жіберілген барлық сұраулар қосылу қателері бар жауаптарды қайтарады.

Егер сіз ата-ана прокси-серверлерінің сәтсіздікке ұшыраған жағдайда сұрау жіберу мүмкіндігін алдын-ала қарастырғыңыз келсе, келесі параметрлерді қолданыңыз:

cache peer parent. com parent 3128 0 no-query prefer direct off nonhierarchical direct off

Баптаулардың екінші жолағы, ата-аналық серверлер қолжетімсіз болса, ағымдағы (бапталып жатқан) серверге қосылу м.үмкіндігін береді. Егер ата-аналық прокси-серверлер қолжетімді болса, олар бірінші арада қолданылады.

Үшінші жолақ Squid-ті ата-аналық прокси-серверлерге, не кэштеуге келмейтін, не тура ағымдағы серверге жөнелту кезінде тезірек өңделетін сұрауларды жіберуге мәжбүрлейді.

<түр> параметрінде жана көршілес прокси-серверді қосу үшін **sibling** мағынасы белгіленеді. Мысалы, егер ағымдағы (бапталып жатқан) қосылыстардың прокси-серверіне **sibling. com** түйін аты бар көршілес прокси-серверін орнату қажет болса, онда прокси-сервердің **squid. conf конфигурациялық файлына келесі жолды қосу қажет:**

cache peer sibling. com sibling 3128 3130

cache_peer_domain директивасы домендерге көршілес және ата-аналық кэштерді тағайындауға мүмкіндік береді. Мысалы, .com домені parent. com ата-аналық кэшын, ал .net домені **sibling. net** көршілес кэшты қолданылуы қажет болса:

cache peer parent. com parent 3128 3130 cache peer sibling.net
sibling 3128 3130 cache peer domain parent. com . com cache
peer domain sibling.net .net

4.4. ҒАЛАМДЫҚ ЖЕЛІЛЕРГЕ ҚОСЫЛУ КЕЗІНДЕГІ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ

Windows Server 2008 R2-де брандмауэрды (Firewall) баптау.

Windows Server 2008 R2 пайдаланушыға қорғанысты қамтамасыз ету құралдарының бүтін комплексін ұсынады. Осындай құралдардың бірі - Windows

(Windows Advanced Firewall) брандмауэры. Бұл бөлімде, ғаламдық желіге қосылу кезіндегі Windows брандмауэрын баптаумен байланысқан бірқатар сұрақтар қарастырылатын болады.

Брандмауэр бейіндері. Windows Server 2008 R2-де пайдаланушыға бейіндердің үш түрі негізінде жұмыс істеу мүмкіндігі беріледі:

1) **домен бейіні** (Domain profile) — сервер Active Directory доменіне қосылған кезде қолданылады;

2) **жеке бейін** (Private profile) — сервер қосымша қорғанысы (мысалы, бағдарлауыш құралдарымен қамтамасыз етілетін) бар жеке желіге жалғанған кезде қолданылады. Бұл бейіннің, домен бейінімен салыстырғанда едәуір қатаң шектеулері болуы тиіс.;

3) **жалпы бейін** (Public profile) — сервер жалпыға ортақ (көпшілік) желіге қосылған кезде қолданылады. Бейіннің бұл түрі үшін ең қатаң шектеулерді қарастыру қажет.

Windows Server 2008 R2-де бейіндер әрбір желілік адаптер үшін бөлек бапталатынын белгілеп кеткен жөн. Бейін, сервер бұл адаптер арқылы қосылу әрекетін жасайтын желі түріне сәйкес анықталады.

Кіріс және шығыс трафикті өңдеу. Windows Server 2008 R2-де Windows брандмауэры әдепкі бойынша барлық кіріс қосылыстар мен трафиктерді, егер бұл қосылыстардың рұқсат ережесі болмаса, бұғаттайды. Барлық шығыс қосылыстар, керісінше, рұқсат етілген. Заманауи брандмауэрлердің көбісінде сияқты, Windows брандмауэры, кіріс қосылыстарды қажет ететін, қандай да бір бағдарламалық жасақтаманы орналастыру (немесе бірінші рет қосу кезінде) кезінде жаңа ереже жасауды ұсынады. Егер де орнатылып жатқан бағдарламалық жасақтама Windows құрамдасы немесе сенілген қосымша болып табылса, онда ереже, пайдаланушының қатысуын талап етпей, автоматты түрде жасалады.

Windows брандмауэрының ережелерін, *Басқару тақтасы/ Жүйе және қауіпсіздік/ Windows брандмауэры/ Қосымша параметрлер* элементі арқылы қол жеткізуге болатын, «Жоғары қауіпсіздік режиміндегі Windows брандмауэры» жабдықтамасында көруге болады.

Қосылуға ережелерді жасау. Жаңа ережені жасау үшін «Жоғары қауіпсіздік режиміндегі Windows брандмауэры» жабдықтамасынан қолжетімді жаңа кіріс қосылыстарға ережелер жасау мастерін қолдануға болады. Мастерді іске қосу үшін Әрекеттер алқасындағы Ережені жасау батырмасын басу қажет.

Мастер жұмысының бірінші қадамында мүмкін төрт нұсқаның ішінен ереже түрін тандау ұсынылады:

1) **бағдарлама** — қосылу әрекетін жасап жатқан бағдарламаға сәйкес қосылуға рұқсат беру үшін. Бұл түрді тандаған кезде ережені жасаудың келесі кезеңінде бағдарламаның орындалып жатқан файлының мекенжайын енгізу қажет.;

2) **порт** — қосылу өткізілетін белгілі бір TCP/UDP порты арқылы қосылуға рұқсат беру үшін. Егер бұл түр таңдалған болса, онда мастердің келесі қадамында порттың нөмірі мен протоколды белгілеу қажет;

3) **алдын-ала анықталған** — тізімдегі бір бағдарлама немесе қызметтің

қосылуына рұқсат беру үшін;

4) **бапталатын** — стандартты типтердің біреуіне де жатпайтын ережелерді жасау үшін.

Егер ереженің бапталған түрі тандалған болса (ереженің, мастер құралдарымен өзгертуге болатын барлық баптаулары қол жетімді болады), онда келесі қадам протоколдар мен порттардың кеңейтілген баптауларына қол жеткізу мүмкіндігін береді.

Келесі қадамда, бұл ереже қолданылатын IP-мекенжайларға жауап беретін, алқаны баптау мүмкіндігі беріледі.

Мастердің келесі қадамы, ереженің шарттарын қанағаттандыратын, кіріс және шығыс пакеттер үшін қолданылуы тиіс, әрекетті тағайындау үшін қолданылады. Содан кейін мастер бұл ереже қолданылатын бейіндерді белгілеуді ұсынады.

Соңғы қадамда ереженің атын және оның сипаттамасын енгізу қажет.

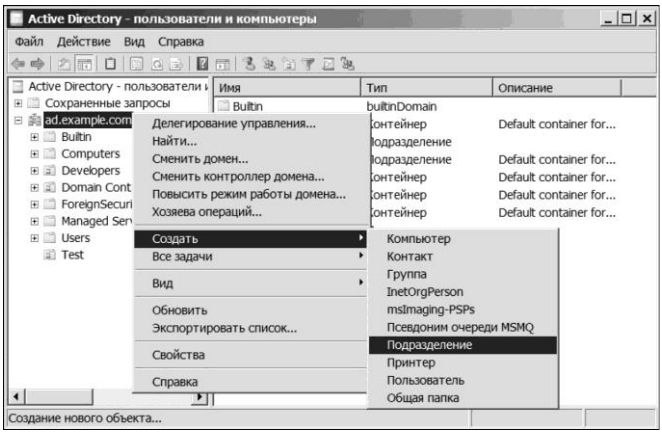
Жасалған ереженің баптауларына рұқсатты, «Жоғары қауіпсіздік режиміндегі Windows брандмауэры» жабдықтамасында, өзгерту қажет болып тұрған ереже үшін мәнмәтіндік мәзірдің *Қасиеттер* тармағын таңдау арқылы қол жеткізуге болады.

Жаңа ережелерді жасаудың мастерінің жұмысы бойынша неғұрлым толық ақпаратты Microsoft TechNet сайтында «Брандмауэр ережелерінің мастері» бөлімінде алуға болады.

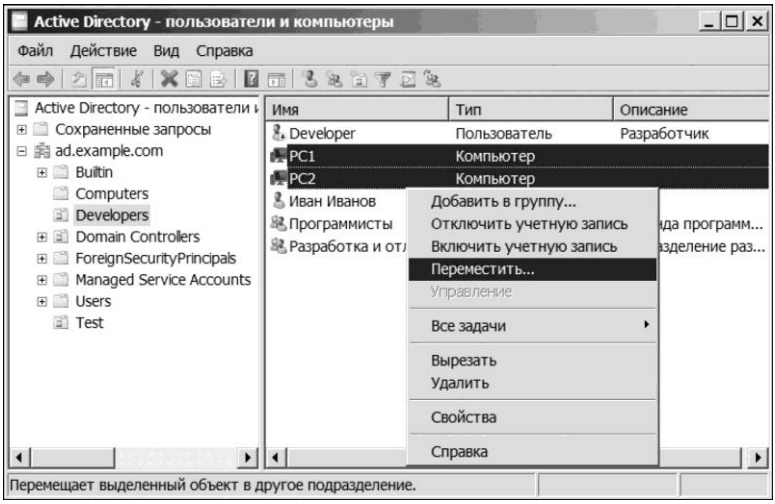
Брандмауэр ережелерін топтық саясат көмегімен басқару. Бүтін бөлімшенің рандмауэрлерін баптау кезінде топтық саясаттарды қолдану әкімшілердің жұмысын бірқатар жеңілдетеді.

Жоғары қауіпсіздік режимінде Windows брандмауэрлерін бақылауға арналған топтық саясат объектісін жасау үшін келесі әрекеттерді орындау қажет:

1) «Active Directory – пайдаланушылар мен компьютерлер» жабдықтамасының көмегімен (*Қосу/Әкімшіліктендіру/ Active Directory – пайдаланушылар мен компьютерлер*), құрастырылып жатқан топтық саясат байланатын бөлімшені құрастыру(егер ондай бөлімше болмаса)(4.5 Сур);



4.5 Сур. «Active Directory – пайдаланушылар мен компьютерлер» жабдықтамасының көмегімен жаңа бөлімшені құрастыру.



4.6 Сур. Объектілерді бөлімшелер арасында алмастыру.

2) пайда болған *Жаңа объект - Бөлімше* диалогтік терезесінде бөлімше атын енгізу және ОК батырмасын басу;

3) жаратылған бөлімшенің мәнмәтіндік мәзірі арқылы «Компьютер» объектілерін құрастыру немесе осыған дейін құрастырылған бөлімшелерден компьютерлерді көшіру (4.6 сур.). Көшіру үшін, көшірілетін объектілерді белгеп, мәнмәтіндік мәзір көмегімен *Көшіру* пәрменін таңдау қажет, содан

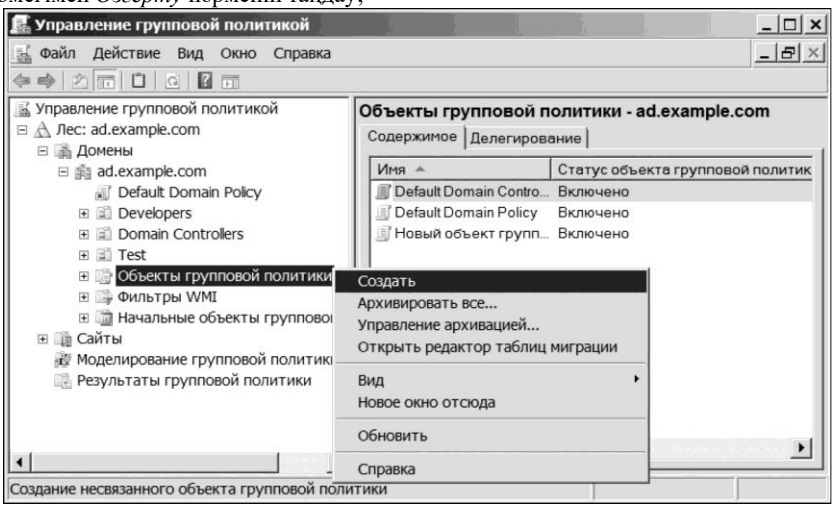
кейін пайда болған терезеде көшіру қажет бөлімшені таңдау қажет;

4) *«Топтық саясатты басқару» жабдықтамасын ашу* (Қосу/Әкімшіліктендіру/ Топтық саясатты басқару) *және Орман түйініне өту:* Орман аты/ Домендер/ Домен аты/ Топтық саясат объектілері;

5) мәнмәтіндік мәзір көмегімен таңдалған түйін үшін *Жасау* пәрменін таңдау (4.7 сур.);

6) пайда болған *Топтық саясаттың жаңа объектісі* диалогтік терезесінде топтық саясаттың жаңа объектісінің атын енгізу және ОК батырмасын басу;

7) топтық саясаттың жаратылған объектісін таңдау және мәнмәтіндік мәзір көмегімен *Өзгерту* пәрменін таңдау;



4.7 сур. Топтық саясаттың жаңа объектісін құрастыру

8) «Топтық саясаттарды басқару редакторында» жабдықтамасында *Компьютер конфигурациясы/ Саясаттар/ Windows конфигурациясы/ Қауіпсіздік параметрлері/ Жоғары қауіпсіздік режиміндегі Windows брандмауэры/ Кіріс қосылыстарға арналған ережелер* түйінін таңдау және мәнмәтіндік мәзір көмегімен *Ережені құрастыру* пәрменін тандау (4.8 сур.).

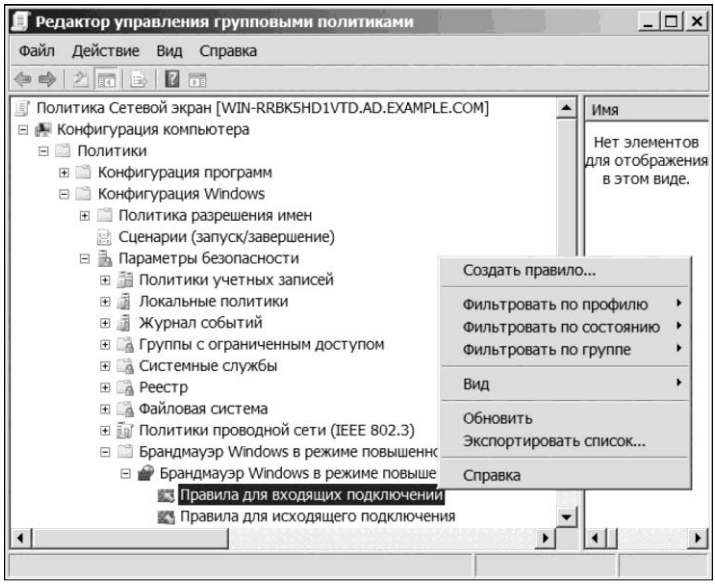
9) «Топтық саясатты басқару» жабдықтамасында ережені баптаудан кейін топтық саясаты бапталатын бөлімшенің түйінің белгілеу, және мәнмәтіндік мәзір көмегімен жаратылған топтық саясат объектісін онымен байланыстыру (4.9. сур).

Желілік мекенжайларды трансляциялау жүйесін баптау (NAT). Network Address Translation (NAT) (желілік мекенжайларды түрлендіру) дегеніміз — бұл, желілер арасында TCP/IP протоколдары арқылы пакеттермен алмасу кезінде IP-мекенжайларды түрлендіруге арналған механизм.

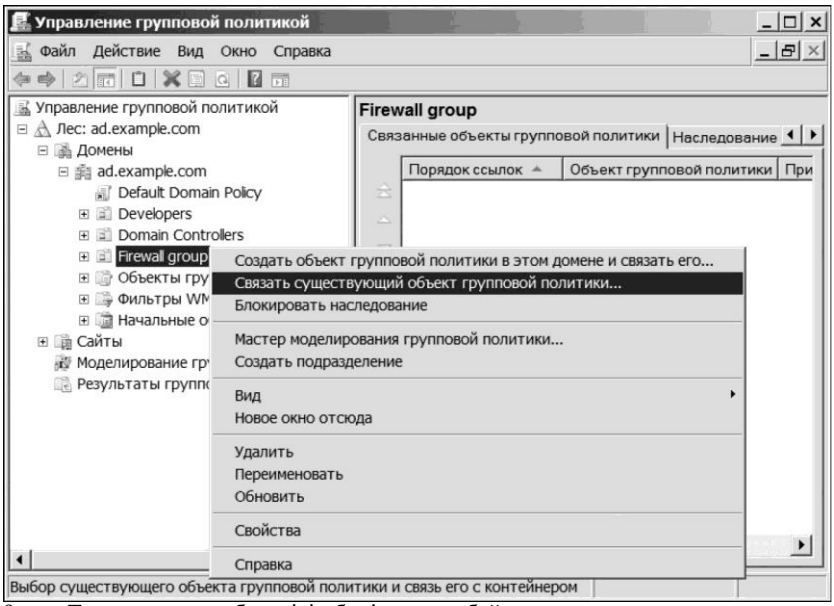
IP-мекенжайлардың трансляциясы келесі нұсқалардың бірі ретінде іске

асырылуы мүмкін:

- **статикалық трансляция** — IP-мекенжайды сыртқы желіден ішкі желінің IP-мекенжайына бірге бір жариялауға мүмкіндік береді;
- **динамикалық трансляция** — IP-мекенжайды сыртқы желіден ішкі желінің небір тобының (мекенжайлар пулының) бір IP-мекенжайына жариялауға мүкіндік береді;
- **порт-мекенжай трансляциясы** — сыртқы желіден IP-мекенжайлардың біршама мөлшерін порттардың әртүрлі мағынасымен ішкі желінің бір IP-мекенжайына трансляциялауға мүмкіндік береді.



4.8 сур. Кіріс қосылыстардың ережелерін құрастыру



4.9 сур. Топтық саясат объектісін бөлімшемен байланыстыру

Желілік мекенжайларды жариялау әдетте қолданылады:

■ IP-мекенжайлардың түрлі диапазондары бар күрілдеуікті қосылған желілер арасында пакеттерді қайта жіберу үшін;

■ ақпаратты жіберуді бақылау және қорғауды, ішкі желі сервистерінің шын мекенжайларды мен порттарын жасыру арқылы қамтамасыз ету үшін;

■ трафикті және ғаламдық желіден қосылыстарды айрықша өңдеу үшін;

■ ішкі желілердің порт-мекенжай трансляциясын қолдану арқылы бір сыртқы мекенжай арқылы жұмысы үшін.

Microsoft Windows Server 2008 R2-де NAT-ты баптау. 4.1 бөлімінде бағдарлауды «Желі мен қолжетімділік саясатының қызметтері» серверінің рөлі көмегімен баптау қарастырылды. Егер, бағдарлау мен қашықтықтан қатынасу осыған дейін мекенжайларды түрлендіру функциясысыз бапталған болса, оларды мастер көмегімен қайта конфигурациялау қажет. Бағдарлау мен қашықтықтан қатынасудың осыған дейін қосылған қызметтерін қайта баптау үшін келесі әрекеттерді орындау қажет:

1) «Бағдарлау және қашықтықтан қатынасу» жабдықтамасын ашу (*Қосу/Әкімшіліктендіру/Бағдарлау және қашықтықтан қатынасу*) және бапталатын серрверге арналған мәнмәтіндік мәзір көмегімен *Бағдарлау мен қашықтықтан қатынасуды өшіру* командасын тандау;

2) пайда болға, оның өшіріліп қалу жағдайында бағдарлау мен қашықтықтан қатынасуды қайта баптау қажеттілігінің ескертуі бар, диалогтік терезеде ОК батырмасын басыңыз.

Қызметтердің өшірілуінен кейін оларды баптауға және қайта қосуға көшуге болады.

Мекенжайларды түрлендіруді баптау үшін келесі әрекеттерді орындау қажет:

1) «Бағдарлау және қашықтықтан қатынасу» консолінің жабдықтамасында бапталатын серверді белгілеу және мәнмәтіндік мәзір көмегімен *Бағдарлау мен қашықтықтан қатынасуды баптау және қосу* командасын таңдау;

2) бағдарлау және қашықтықтан қатынасу серверін баптау мастерінің бірінші бетінде *Әрі қарай* батырмасын басу;

3) егер серверді тек желілік мекенжайларды түрлендіруге баптау қажет болса, онда конфигурацияны таңдау бетінде *Желілік мекенжайларды түрлендіру (NAT)* тармағын тандау қажет. Егер де қызмет қосымша функцияларды қолданатын болса, онда *Ерекше конфигурация* тармағын тандау және қажетті функцияларды орнату қажет;

4) мастер жұмысының келесі кезеңінде NAT негізінде Интернетке қосылуды баптау қажет. Ғаламдық желіге кіру іске асырылатын интерфейсті тандау қажет;

5) мастер жұмысының келесі кезеңінде, мекенжайлардың тағайындалуы мен аттардың салыстырылуы NAT құралдарымен қамтамасыз етілетіндігін немесе қамтамасыз етілмейтіндігін тандау қажет. Егер желіде статикалық IP-мекенжайлар қолданылатын болса немесе бұл функцияларды қамтамасыз ететін серверлар бар болса, онда *аттар мен мекенжайларды салыстыру қызметтерін кейінірек орнату* тармағын таңдау қажет**;**

6) мастер жұмысының қорытынды кезеңінде *Дайын* батырмасын басу қажет.

«Бағдарлау және қашықтықтан қатынасу» жабдықтамасында мастердің жұмысының аяқталуынан кейін баптаулы сервердің **IPv4** түйінінде *Желілік мекенжайларды түрлендіру (NAT)* түйіні пайда болады.

Желілік мекенжайларды түрлендірудің баптауларын өзгерту үшін *Желілік мекенжайларды түрлендіру (NAT)* түйінін таңдап, мәнмәтіндік мәзір көмегімен *Қасиеттер* командасын таңдау қажет. Пайда болған *Қасиеттер: Желілік мекенжайларды түрлендіру (NAT)* терезесінде шешілетін тапсырмаға сәйкес қызметті баптау қажет.

Мекенжайларды түрлендірудің қасиеттер терезесінің *Мекенжайларды тағайындау* қосымша беті *Желілік мекенжайларды түрлендіру (NAT)* құрамдасының құралдары арқылы мекенжайлардың автоматты түрде тағайындалуын баптауға м.мкіндік береді. *Мекенжайлардың тағайындалуы* қосымша бетінің *Болдырмау* батырмасы, одан әрі автоматты түрде тағайындалу мүмкіндігі болмайтын кейінге сақталған мекенжайларды қосуға арналған.

Интернетке кіру жоспарланатын интерфейсті баптау үшін келесі әрекеттерді орындау қажет:

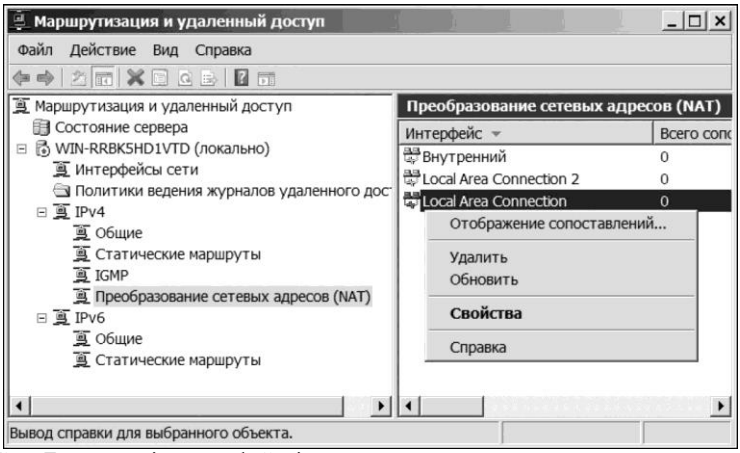
1) «Бағдарлау және қашықтықтан қатынасу» жабдықтамасында бапталатын серверге арналған *Желілік мекенжайларды түрлендіру* түйінін тандау және қолжетімді жүйелік интерфейстердің арасынан, ғаламдық желіге кіру ұйымдастырылатын интерфейсті таңдау (4.10 сур.);

2) бапталатын интерфейске арналған мәнсмәтіндік мәзір көмегімен

Қасиеттер пәрменін таңдау;

3) егер NAT қолдауы қосылмаған болса, оны қосу;

4) *Мекенжайлар пулы* қосымша бетінде, сыртқы интерфейске байланған мекенжайларды, *Қосу* батырмасының көмегімен қосу. Мекенжайлар пулын енгізуге арналған терезенің, толтыруға арналған үш өрісі бар: *Бастапқы мекенжай, Соңғы мекенжай* және *Маска.* Осындай түрмен қосылған мекенжайлар пулы 192.168.0.10 және 192.168.0.15 IP-мекенжайларына ие болады;



4.10. Сур. Баптау үшін интерфейсті таңдау

5) Қызметтер және порттар қосымша бетінде, желілік мекенжайларды түрлендіру сервері арқылы жария етуге болатын, протоколдарды баптау. Мысалы, **Web- сервер (HTTP) протоколын баптау қажет. Таңдалған протоколға басқан кезде оның баптаулар әйнегі ашылады (4.11 сур.)**

Жеке желідегі мекенжай дегеніміз – бұл, сыртқы желіден келетін сұрауларды HTTP протоколы, 192.168.0.12 мекенжайы және TCP 80 порты арқылы өңдейтін ішкі мекенжай.

Мөлдір проксилеуді баптау (transparent proxy).

Мөлдір проксилеу деп, клиент сыртқы желіге сауал жібере отырып кэштейтін сервиспен қосылатын проки-сервердің байланыс тәсілін атайды. Осындай қосылыс кезінде клиент құрылғысында проксиді баптау қажет етілмейді. Оның орнына қосылыстарды прокси-серверге брандмауэр немесе бағыттағыш арқылы қайта ба.ыттау қолданылаады.

Мөлдір проксилеуді ұйымдастырудың нұсқаларының бірі болып, сыртқы желінің Web-серверлеріне жүгінетін клиенттердің барлық сауалдарын прокси-серверге қайта бағыттауға арналған, мөлдір HTTP-прокси болып табылады. Осы кезінде прокси-қосылыстардың (жүйенің барлық сервистері үшін әдепкі түрде

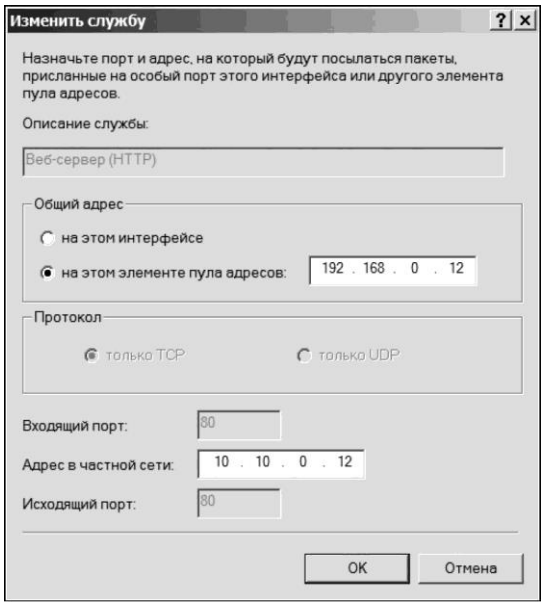
қолданылатын) жүйелік баптаулары да, сыртқы сервистерге кіруге қолданылатын (мысалы, брандмауэрлердегі), бағдарламалардағы проксилердің баптаулары да қажет етілмейді.

Мөлдір HTTP-проксиін ұйымдастыру кезінде, қосылыстар мен трафикті қайта бағыттаудың келесі қырларын ескеру қажет:

- Прокси-серверді орнату және қосылыстарды қабылдау және өңдеуге баптау;
- кэш-серверді ішкі желінің кез келген IP-мекенжайынан 80 порт арқылы қайта бағытталған пакеттерді қабылдауына баптау;
- қайта бағытталған пакеттердің прокси-серверге жеткізілуін қамтамасыз ету. Linux жүйесінде бұл жүйенің ядросы арқылы жүзеге асырылады, Windows жүйелеріне арнайы қосымшалармен трафикті қайта бағыттау қажет, мысалы, бұл функциясы бар бар брандмауэрлар арқылы. Егер прокси-сервері барлық пакеттер ішкі және сыртқы желі арасында өтетін құрылғыда орналастырылған болса (мысалы, маршрутизатор), онда пакетті жеткізу функциясы аппараттық құралда іске асырылуы мүмкін.

4.3 бөлімінде Squid прокси-серверінің бапталуы қарастырылды. Squid мөлдір проксилеу режимінде жұмыс істеуі үшін, **squid.conf** конфигурациялық файлына келесі жолдарды қосу қажет:

acl intranet src 192.168.1.0/24 #ішкі желі http port 3128 transparent



5.2. Сурет. Web-сервер аудитінің конфигурация қосылуы

Алайда пакеттердің бұл (3128) портқа қайта жіберілуін ұйымдастыруды ескеру қажет. Linux-жүйелерінде бұл, IP Filtering/Forwarding функциялары арқылы іске асырылады.

БАҚЫЛАУ СҰРАҚТАРЫ

1. Бағдарлау дегеніміз не?
2. Бағытты анықтау қалай өтеді?
3. Бағдарлау кестесіне қандай ақпарат кіреді?
4. Коммутация алгоритмі қандай?
5. Статикалық және динамикалық бағдарлау арасындағы айырмашылық қандай?
6. Бағдарлау алгоритмі қандай белгілер бойынша жіктеледі?
7. Windows Server 2008-дегі динамикалық бағдарлауды баптау қалай өтеді?
8. Wi-Fi кіру нүктесі дегеніміз не?
9. Infrastructure режимінің қандай жұмыс нұсқаларын білесіз?
10. Сымсыз желіні кіру нүктесін қолданып жазу калай өтеді?
11. Squid кэштейтін прокси-сервері қандай платформаларда жұмыс істей алады?
12. Squid прокси-серверін жаю үрдісінің мәні неде?
13. Кіруді бақылау тізімі не үшін қажет?
14. Кіруді бақылау тізімінде жазылған ережелер бойынша өтінімдерді тексеру қалай іске асырылады?
15. Squid-та аутентификацияның қандай сұлбалары қолданылады?
16. Прокси-серверлердің баспалдақтарын қолданудың өзгешелігі неде?
17. Windows Server 2008 брандмауерінің қандай бейіндері сізге белгілі?
18. Windows Server 2008 брандмауерінің кіріс/шығыс трафиктерін өңдеудің логикасы қандай?
19. Windows Server 2008 қосылуына арналған ережелер қалай құрастырылады?
20. Брандмауерді баптау кезіндегі топтық саясатты қолданудың ыңғайлылыға неде?
21. IP-мекен жайларды трансляциялаудың қандай нұсқалары сізге белгілі?
22. Желілік мекен-жайларды трансляциялаудың негізгі мақсаттары қандай?
23. Мөлдір проксилеу дегеніміз не?
24. Мөлдір HTTP-проксиді ұйымдастыру кезінде қандай ерекшеліктерді ескеру қажет?

5 тарау

ФАЙЛДЫҚ СЕРВЕР, ПОШТАЛЫҚ СЕРВЕР, SQL-СЕРВЕР, WEB-СЕРВЕРДІ ПАЙДАЛАНУҒА СҮЙЕМЕЛДЕУ ЖӘНЕ БАҚЫЛАУ

5.1. WEB-СЕРВЕРДІ СҮЙЕМЕЛДЕУ ЖӘНЕ БАҚЫЛАУ

Web-серверді сүйемелдеу ары қарай MicrosoftWindowsServer2008 R2 жүйесінде жайылған MicrosoftIIS сервер рөлінің негізгі құрамдас бөлігі (Web-сервер) мысалында қарастырылатын болады.

InternetInformationServices (IIS) — бұл әр түрлі бағыттағы интернет-серверлерді өңдеу, өрістету және сүйемелдеуге арналған платформа.

Web-сервердің құрамдас бөлігі Web-серверді құру, өрістету, сүйемелдеу және басқару құралдарын ұсынады.

Сервер конфигурациясын бақылау. Web-сервер әкімшісінің алдында жиі-жиі сервер конфигурациясын өзгерту мониторингінің тапсырмасы тұрады. Бұл конфигурация өзгертулеріне қол жетімділігі бар сценарийдің жұмыс істеу қабілеттілігіне тексеру немесе сервер әкімшілері болып табылмайтын пайдаланушылар оған қол жеткізе алғанда конфигурация өзгерістерінің қадағалануын қамтамасыз ету болуы мүмкін.

Осындай аудит жүргізген кезде конфигурацияны кім өзгерткенін, нақты не өзгертілді және оны қалай түзету керектігін (егер өзгерту жағымсыз салдарға әкеп соқса) білу қажет.

IIS қызметтерінің конфигурациясы мәтіндік XML-файлдар арқылы басқарылады.

Конфигурацияның әр файлы белгілі бір сервиске (сайт, қосымша және т.б.) жатады.

IIS құрамдас бөліктерінің конфигурациялары келесі XML-файлдарда сақталады:

- *Machine. config*— бүкіл сервердің баптаулары бар;
- *ApplicationHost. config*— компьютер конфигурацияларын сақтайды;

Web. config— Web- торап, каталог сияқты объектілерге арналған баптаулары бар.

Machine. config файлында жатқан баптаулар IIS конфигурацияларының файлдарын қоса, конфигурацияның барлық қалған файлдарын иемденеді.

Деректер сервері деңгейінде конфигурациялық файлдар келесі директорияларда сақталады:

- Machine. config *және* Web. config *(негізгі)* - Windows/Microsoft.NET/Framework/< framework нұсқасы>/ CONFIG\;

каталогында табуға болады.

- ApplicationHost. config — Windows/system32/inetsrv/ config/ каталогында табуға болады.

Web. config файлын сервер деңгейінен иемденетін файлдардан ерекшеленетін баптауларды сақтау үшін пайдалануға болады. Бұл файл басқарылатын объектінің ішіндегілері (каталог, сайт немесе қосымша) сақталатын каталогтарда сақталады.

Бас деңгейдегі *Web. Config* файлы параметр баптауларына қол жетімділігін шектеу мақсатында конфигурацияның еншілес объектісін көрсету үшін пайдаланылуы мүмкін.

Конфигурация объектілері сервер деңгейіндегі конфигурация файлдарынан немесе конфигурацияның бас файлдарынан конфигурация параметрлерін иемденеді.

Конфигурацияны ұсыну жергілікті компьютерде әкімші құқықтарына иелік етпейтін пайдаланушыларға белгілі бір конфигурация файлдарын әкімшілендіруге мүмкіндік береді. Бұл үшін IIS7 қызметтерінде конфигурация блоктау/блоктан шығару бөлімдері пайдаланылады (үнсіз келісім бойынша барлық бөлімдер блокталған және тек жүйе әкімшісімен сервер деңгейінде өзгертіледі).

Конфигурация файлдарын редакциялау. IIS конфигурация файлдарын бірнеше әдіспен редакциялауға болады. Мысалы:

1) Конфигурация редакторының көмегімен. Конфигурация редакторы IIS диспечерінің интерфейсі арқылы конфигурация файлдарын басқаруға арналған. Конфигурация редакторын IIS *қызметтерінің диспечерінде (Қосу/Әкімшілендіру/*IIS *қызметтер диспечері*) тауып алуға болады. Конфигурация редакторын шақыру үшін конфигурация объектісінің торабын белгілеп, *Басқару* тұсында *Конфигурация редакторы* элементін таңдау қажет*;*
2) XML-редакторы арқылы немесе мәтіндік процессор көмегімен.

Конфигурация файлдарының қауіпсіздігі конфигурация табыстауын түзу пайдалану және конфигурация бөлімдерін блоктау жолымен қамтамасыз етіледі.

*Windowsв IIS7 басқару аспаптары.*WindowsManagementInstrumentation (WMI) орталықтандырып басқару және компоненттерін байқауға арналған.

IIS7-де осы технология келесі тапсырмаларды шешу үшін пайдаланылуы мүмкін:

- Web-сервер конфигурациясының файлдарын оқу және өзгерту;
- модульдерді басқару;
- Web-сервер құрамдас бөліктерін баптау;
- сайттардың мониторингі мен диагностикасы

WMI пайдаланған кезде қойылған тапсырмаларды шешу үшін құқықтардың табысталуын қарастыру қажет.

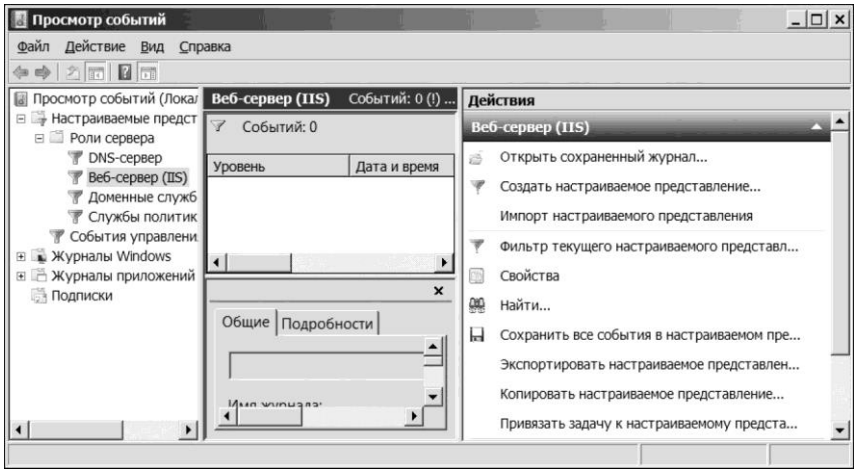
Оқиғалар журналын жүргізу. Осы атқарым Web-сервердің жай-күйін мониторингтеу кезінде пайдалы Web-серверге сауалдар журналын енгізуге арналған.

Web-сервер оқиғаларын журналдау баптауларына қол жетімділігін IIS

қызметтер диспечерінде алуға болады. Журнал жүргізуді баптау үшін IIS қызметтер диспечерінде конфигурацияланған торап үшін «Журнал жүргізу» атқарымын ашу қажет.

Журналды қарау үшін «Оқиғаларды қарау» бағдарламасын пайдалану қажет. Ол *Қосу (Әкімшілендіру/Оқиғаларды қарау* мәзірі арқылы ашылуы мүмкін (5.1-сурет). Ағаш объектісінде Web-сервер оқиғаларын қарау үшін *Бапталатын ұсынулар/Сервер рөлдері/Web- сервер* (IIS) торабын таңдау қажет.

Web-сервер конфигурациясының аудиті. Web-сервер конфигурациясына бақылау жасаудың екінші нұсқасы сервер конфигурациясын өзгерту оқиғаларын байқап отыру болып табылады. Осы атқарым оқиғалар журналын жүргізуге мүмкіндік береді және оның әрқайсысы үшін мына ақпараттан тұратын жазба құрылады:



5.1-сурет. «Оқиғаларды қарау» бағдарламасы

- Web-сервердің конфигурациясын кім өзгертті;
- конфигурацияның қай элементі өзгертілді;
- қандай өзгертулер енгізілді;
- өзгертілген параметрлердің бастапқы мәні.

Web-сервер конфигурациясының аудитін қосу үшін мына іс-әрекеттерді орындау қажет:

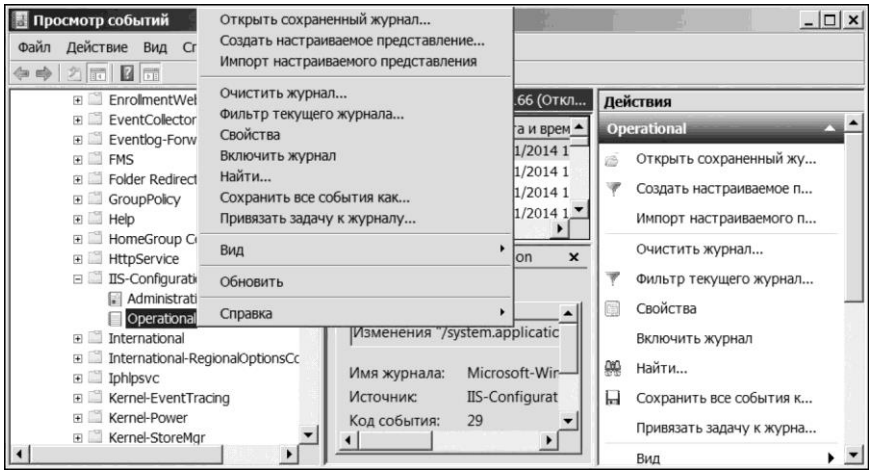
1) *Қосу (Әкімшілендіру/Оқиғаларды қарау* мәзірінде көпшілікке қол жетімді «Оқиғаларды қарау» бағдарламасын ашу;
2) Элементтер ағашында */Microsoft/Windows/IIS-configuration қызметтері мен қосымшаларының журналдары* (5.2-сурет) торабын ашып, мәнмәтіндік мәзір көмегімен *Operational* элементі үшін *Қосу* командасын таңдау.

Қажет болған жағдайда *Қасиеттер* мәнмәтіндік мәзірінің командасы арқылы қол жетімді оқиғалар журналының қасиеттерін баптау мүмкіндігі бар. Журналдың

максималды мөлшерін, журнал файлына жол салу және басқа да опцияларды сұрауға болады.

Web-сервер конфигурациясын өзгерту журналына жазылатын әр оқиғаның құрамында келесі ақпарат бар:

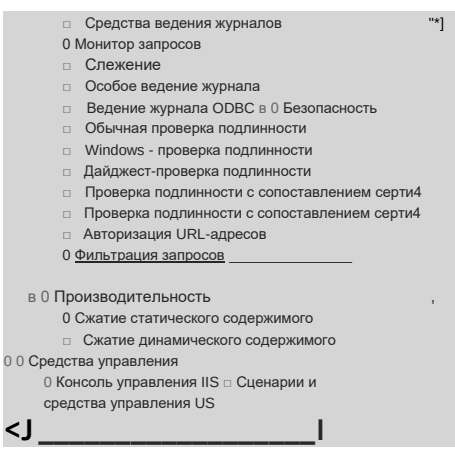
- Конфигурацияға қол жетімділігін алған процессордың нөмірі (ProcessID— PID);
- Өзгертуді жасаған пайдаланушының нөмірі (SecurityIdentifier— SID);

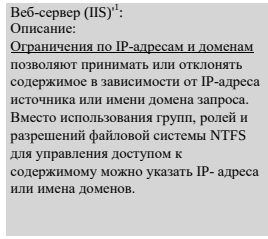


5.3-сурет. IIS қызметтерін орнатқан кезде *IP-мекенжайлар мен домендерді шектеу* құрамдас бөлігін таңдау

IP-мекенжайлар мен домендер бойынша шектеулерді баптау. Рұқсат ету немесе тыйым салу жаңа элементтерін қосу үшін мына іс-әрекеттерді орындау қажет:

1) *Қосу/Әкімшілендіру/ IIS қызметтерінің диспечері* мәзірінің тармағы арқылы «IIS қызметтерінің диспечерін» ашу;
2) IIS қызметтер диспечерінің ағашынан бапталатын элементті таңдау және бапталатын объектінің *IIS* тобында жатқан *IP-мекенжайлар мен домендер бойынша шектеулер* атқарымын ашу;
3) *IP-мекенжайлар мен домендер бойынша шектеулер* интерфейсінде *Іс-*





әрекеттер тұсындағы қосылатын элемент типін таңдау; таңдалған шектеу элементіне басқан кезде қосылатын шектеу (таңдаған элементке

■ жасалған өзгертулер туралы мәлімет.

Осы журналды жүргізу арқылы конфигурация файлдарының деңгейінде қол жетімділігі жүзеге асырылатын болса, Web-сервер конфигурациясында жасалған өзгертулерді байқау мүмкін емес.

Серверге қол жетімділігін шектеу. MicrosoftIIS7 платформасы IP-мекенжайлар бойынша серверге қол жетімділігін шектеу құралдарын ұсынады. Бұл жағдай серверге сұрау салу талдауы негізінде әкімшіге Web-сервердің сервисіне қол жетімділігін шектеуді баптауға мүмкіндік береді. Осындай талдау астында IP-мекенжайлардың сенімсіз белсенділігін іздеу жатыр.

Сенімсіз IP-мекенжайларды іздеу процессі оқиғалар журналын тадауға мүмкіндік беретін әр түрлі бағдарламалық құралдар арқылы автоматтандырылуы мүмкін.

«IP-мекенжайлар мен домендер бойынша шектеу» құрамдас бөлігін орнату. «IP-мекенжайлар мен домендер бойынша шектеу» құрамдас бөлігін орнату үшін *Web-сервер (IIS) сервер рөлін орнатқан кезде осы құрамдас бөлікті (5.3-сурет) немесе* IISc қызметтерін орнатқаннан кейін рөлдер қызметін қосу арқылы таңдау қажет.

байланысты рұқсат беретін немесе тыйым салатын) ережелерін баптау терезесі шығады. Бұнда белгілі IP-мекенжай өрісін немесе бүркемесін көрсетумен мекенжайлар ауқымын толтырып, ОК батырмасын басу.

Шектеу тізімінде көрсетілмеген клиенттердің қол жеткізу параметрлерін баптау *IP-мекенжайлар мен домендер бойынша шектеулер* атқарымының *Іс-әрекеттер* тұсындағы *Параметрлерді өзгерту* элементінің көмегімен өтеді. Қол жеткізе алатын екі нұсқаның бірін таңдау қажет:

1) *Рұқсат беру* — барлық клиенттердің қол жетімділігіне рұқсат беру, тек тыйым салу ережесінде шектеуі барларды қоспағанда;
2) *Тыйым салу* — барлық клиенттердің қол жетімділігіне тыйым салу, тек рұқсат беру ережесінде көрсетілген клиенттерді қоспағанда.

Бас объектінің шектеулер ережелерінің баптауларын қайтарып алу үшін *IP-мекенжайлар мен домендер бойынша шектеулер* атқарымының *Іс-әрекеттер* тұсындағы *Бас параметрлерге қайтару* элементін таңдау қажет.

IIS8-де *IP-мекенжайлар мен домендер бойынша шектеулер* атқарымында IP-мекенжайларды динамикалық сүзгілеу баптауларының мүмкіндігі қосылған болатын. Бұл серверге көп сұрау салатын IP-мекенжайлардың блоктауын баптауға мүмкіндік береді.

Деректер берілімін оңтайландыру. Деректер берілімін оңтайландыру шығару деректерін кэштеу технологиясын пайдалануды қарастырады.

Шығару деректерін кэштеу ақпараттарға жүгіну серверді шамадан артық пайдаланатын осы ақпаратты сақтау есебінен Web-сервердің өнімділігін арттыру үшін қолданылады. Кэштелген деректер Web-сервердің жаднамасында сақталады және клиенттерге осы ресурстерге қайтадан жүгінген кезде қайтарылады. Бұл сұрау салған сайын Web-парақтарды қайтадан өңдеу қажеттілігін жояды.

Web-серверді ұйымдастырған кезде кэштелетін ақпарат сипаттамасы мен ашылатын жабдықтың аппараттық ресурстарына (жедел жад ресурстарына) назар салу қажет. Себебі бұл ақпарат сервер жадында сақталады.

Кэштелген ақпаратқа мысал ретінде сервермен сыртқы көздерден, мысалы деректер қоры немесе басқа да сақтау орындарынан алынған деректерді пайдалануа болады. Сондағы өнімділік ысырабы Web-сервермен қоса деректер қорына қызмет көрсететін серверді де қозғайды. Web-сервер кэшінде көбінесе жиі қойылатын сұраулардың нәтижелерін сақтап, осы ақпаратты пайдаланушылардың талабы бойынша беріп отырған жөн. Кэштеуге қажетті деректердің тағы бір мысалы пайдаланушылардың көбімен алынатын статикалық және бірдей, алайда Web-сервер тарапынан күрделі немесе ұзақ өңдеуді талап ететін ақпарат болып табылады.

MicrosoftIIS қызметтерінің құралдарымен деректерді кэштеуге баптау. Шығару деректерін кэштеуге қосу және баптау үшін мына іс-әрекеттерді орындау қажет:

1) *«IIS қызметтерінің диспечерін»* (Қосу/Әкімшілендіру/IIS қызметтерінің диспечерін) ашу;
2) Баптау жүргізілетін торапты таңдау;

3) *IIS мүмкіншіліктерін қарау тобында Шығару деректерін кэштеу атқарымын ашу;*
4) Шығару деректерін кэштеу *интерфейсінде* Іс-әрекеттер *панеліндегі* Өзгерту *батырмасын басу;*
5) Пайда болған Шығару кэшінің баптауларын өзгерту сұхбат терезесінде Кэшті қосу опциясын таңдап, ОК батырмасын басу.

Жауаптар кэшінің ең үлкен мөлшері (байттарда) өрісі кэштелген жауаптардың ең үлкен мөлшерін баптауға жауап береді. Үнсіз келісім бойынша осы параметрдің 256 Кбайт мәні бар.

Кэштің шекті мөлшері (мегабайттарда) өрісін қосқан жағдайда кэштелген шығару ақпараты үшін жаднама пайдаланатын ресурстерінің көлемін шектеуге мүмкіндік береді. Егер өрісінде «0» көрсетілсе (үнсіз келісім бойынша), IIS қызметтері осы параметрді автоматты түрде басқарады.

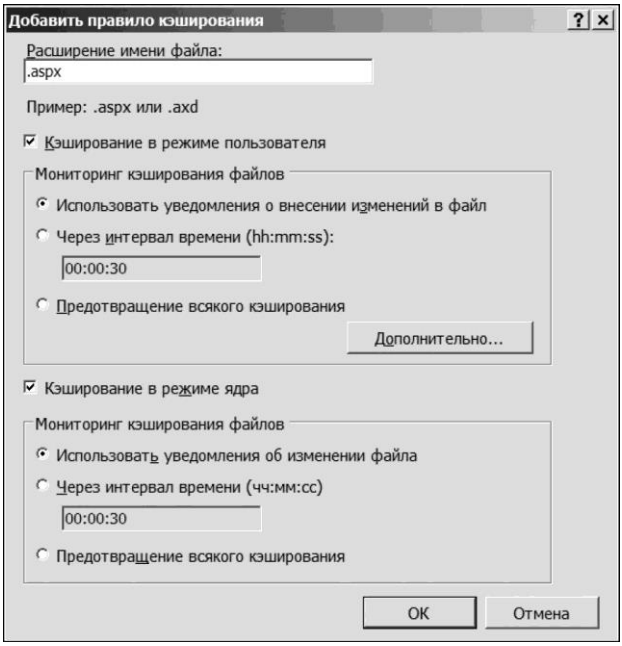
IIS қызметтеріндегі шығару деректерді кэштеу ережелері. Кэштеу ережелері енгізілген ақпарат типімен ерекшеленетін сұраулар топтарын белгілеу есебінен кэштелген ақпараттарды икемді басқаруға мүмкіндік береді. Бұндай амал, мысалы, күрделі өңдеуді талап ететін ақпаратты ұзағырақ сақтауға және кэшті динамикалық өзгертілетін кэштелген деректерден жиі тазалап тұруға мүмкіндік береді.

Шығару деректерін кэштеудің жаңа ережесін құру үшін мына іс-әрекеттерді орындау қажет:

1) *«IIS қызметтерінің диспечерін»* (Қосу/Әкімшілендіру/IIS қызметтерінің диспечерін) ашу;
2) Баптау жүргізілетін торапты таңдау;
3) *IIS* мүмкіншіліктерін қарау тобында *Шығару деректерін кэштеу* атқарымын ашу;
4) *Іс-әрекеттер* панеліндегі *Қосу* батырмасын басу;
5) Пайда болған *Кэштеу ережесін қосу* сұхбат терезесінде *Файл атауын кеңейту* өрісінде ереже құрылатын файлдың кеңейтілімін енгізу, сонымен қатар басқа параметрлерді баптау (5.4-сурет).

Кэштеу ережесін құрған кезде келесі параметрлерді баптауға болады:

а) *Пайдаланушы режимінде кэштеу* опциясы — шығару деректерін кэштеуге жауап береді. Кэштеу мониторингінің келесі нұсқаларының бірін болжайды::


Добавить правило кэширования
Расширение имени файла:
.aspx
Пример: .aspx или .axd
Кэширование в режиме пользователя
Мониторинг кэширования файлов
Использовать уведомления о внесении изменений в файл
Через интервал времени (hh:mm:ss):
00:00:30
Предотвращение всякого кэширования
Дополнительно...
Кэширование в режиме ядра
Мониторинг кэширования файлов
Использовать уведомления об изменении файла
Через интервал времени (чч:мм:сс)
00:00:30
Предотвращение всякого кэширования
OK
Отмена

- *Файлдың өзгеруі туралы хабарландыруды пайдалану* — қажетсіздіктен кэш ішінен өзгертілген ақпаратты жоюға мүмкіндік береді;
- *Уақыт аралығы арқылы (hh:mm:ss)*— кэштен ақпаратты жолда белгіленген уақыт аралығынан кейін жоюға мүмкіндік береді;
- *Әрбір кэштеудің алдын-алу* — бұл нұсқаны таңдау белгіленген кеңейтуден әрбір кэтеуге шектеу қояды;

б) *Алдын-ала кэштеу тәртібі опциясы* — алдын-ала тәртібінде қосымша кэштеуді қолдануға мүмкіндік береді. Файлдарды кэштеу мониторингінің нұсқалары пайдаланушы тәртібінде кэштеумен ұқсас. Бірақ, алдын-ала тәртібінде кэштеу кезіндегі баптаулар пайдаланушы тәртібінде көрсетілген кэштеуге бөгет жасайды.

Пайдаланушы тәртібінде кэштеудің бақылау параметрлері ішіндегі *Қосымша* түймесін басқан кезде *шығару кэші үшін ереженің қосымша параметрлері* диалогтік терезесі ашылады. Берілген терезеде динамикалық парақшаларды кэштеу үшін қолданылатын сұраныстарды айнымалы жолдарын баптау мүмкінділігі ұсынылады.

Динамикалық түрде құрастырылған парақшалар кэштеудің басқа тәсілін талап етеді.егер, статикалық парақшалар көбіне бастапқы орнатулар бойынша (Web-сервердің жады ресурстарының қоры жеткілікті болған жағдайда) кэштелетін болса, динамикалық парақшаларды кэштеу міндетті емес. Кэштеу міндетті емес динамикалық парақшалар мысалы ретінде әрбір ерекше клиент үшін ерекше болатын (нақты уақыт аралығында) интернет-дүкендерінің каталогтары көрсетуге болады. Мұндай парақшаларды кэштеудің қажеті жоқ. Бірақ, динамикалық парақшаларды кэштеу көбіне орынды болып табылады, мысалы, бірден өзгеретін контенті бар, бірақ, пайдаланушымен ыңғайлы интерфейс үшін динамикалық түрде үйлесетін парақшалар үшін.

5.2. ФАЙЛДЫҚ СЕРВЕРДІ СҮЙЕМЕЛДЕУ ЖӘНЕ БАҚЫЛАУ

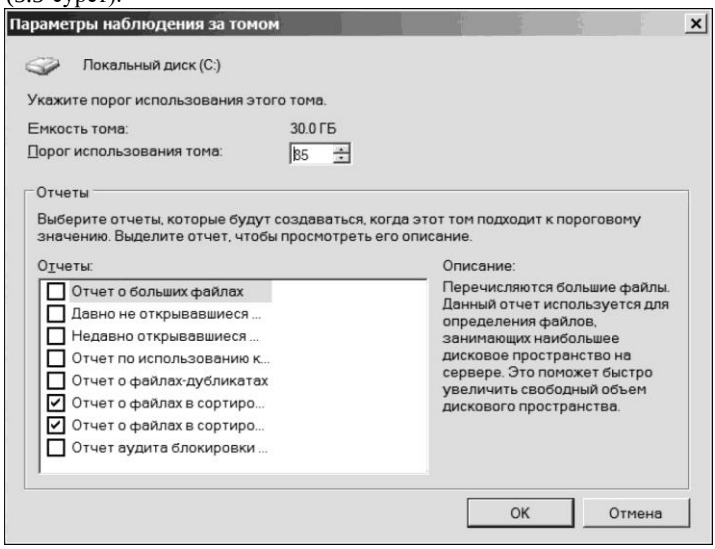
Файлдық сервер келесі міндеттерді атқару үшін тағайындалған:

- Дискілік үлестерді басқару;
- Индекстеуді басқару;

- Сервердің жалпы ресурстарын басқару;
- Қолжетімділікті және т.б. басқару.

Сервер конфигурациясын бақылау. MicrosoftWindowsServer2008 R2 жүйесінде файлдық сервердің рөлін орнату үшін келесі әрекеттерді орындау қажет:

1) «Сервер диспетчерін» ашу және мәнмәтін мәзірі көмегімен *Рөл* торабы үшін *Рөл қосу* командасын таңдау – рөлдерді қосу терезесі ашылады;
2) Қосылатын рөлдер терезесінде *Файлдық қызметтер* тармағын таңдаңыз және *Ары қарай түймесін басыңыз;*
3) *Рөл қызметтерін таңдау* терезесінде файлдық сервер алдында қойылған тапсырмаларды орындау үшін қажет болатын қызметтерді көрсету қажет. Егер, қосымша қызметтер таңдалған болса (файлдық серверден басқа), кейбір қызметтер параметрлерін көрсету қажет болады. Ары қарай *Файлдық сервердің ресурстар диспетчері* опциясы бар файлдық серверді орнату қарастырылады;
4) Келесі *Сақтау жерін бақылау* терезесінде бақылау жүргізу қажет болатын томдарды көрсету қажет. *Томдарды бақылау параметрлері* терезесіндегі *Параметрлер* түймесі томды пайдалану шегін баптауға және осы шектік мәнге жеткен уақытта құрылатын есептілік түрлерін таңдауға көмек береді (5.5-сурет).



5) Келесі кезеңде есептіліктерді сақтау жолын таңдауды немесе есептіліктерді электрондық пошта құралдарыменен көрсетілген мекенжайға есептіліктерді жіберуді таңдауды талап ететін *есептілік параметрлері* терезесі ашылады;
6) шебердің аяқтаушы қадамында *Орнату* батырмасын басыңыз.

Файлдық серверді баптау. WindowsServer2008 R2 жүйесіндегі файлдық серверді баптау *Іске қосу//Әкімшілендіру* немесе сервер диспетчерінен (*Файлдық қызметтер* торабы) қолжетімді *Жалпы ресурстар мен сақтау орнын басқару*

құрауыштар құралымен жүзеге асырылады.

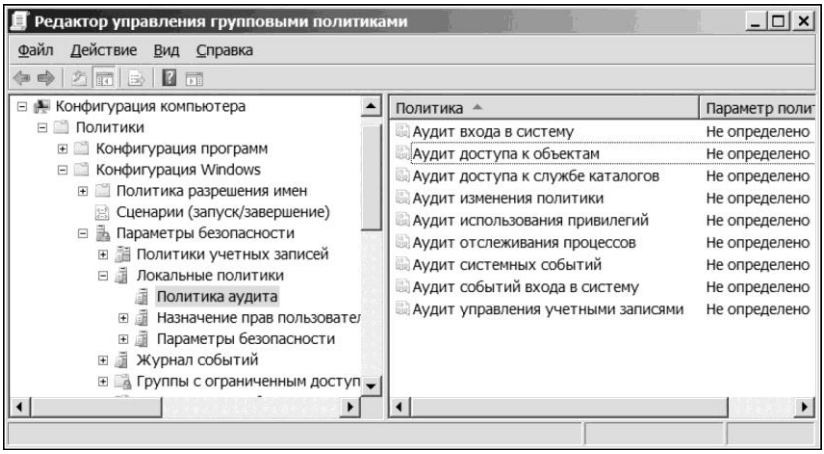
Файлдық сервер аудитін басптау. Файлдық сервер аудиті жалпы ресурстардың өзгерістерін қадағалаумен байланысты бірқатар тапсырмаларды шешуге мүкіндік береді, сонымен қатар: файлдар өзгерісін (редакциялау, жою, құру және т.б.) қадағалау; жалпы ресурстарды кім және қашан өзгерткенін қадағалау. Берілген тапсырмалар жалпы ресурстар әдетте осы ресурстардың барлық пайдаланушыларына қолжетімді болатындығынан туындайды. Файлдарды өзгерту жағымсыз салдарға алып келуі мүмкін жағдайлар туындауы мүмкін, мысалы, құжатты жойғаннан немесе қате өзгеріс енгізгеннен мекеменің бизнес-процесі құлдырады. Мұндай жағдайда процестің қызметін тез арада қайта қалпына келтіру үшін құжатқа қате өзгерістерді кім енгізгенін және қандай өзгерістер енгізілгенін білу қажет.

Файлдық сервердің бақылауы сервердің файлдық ресурстарына қолжетімділік аудитінің кеңейтілген баптауын қарастырады.

Жалпы ресурстардың аудитін баптау үшін келесі әрекеттерді орындау қажет:

1) жалпы ресурстар қасиеттерін ашыңыз және *Қауіпсіздік* қосымша бетінде қауіпсіздіктің қосымша параметрлерін ашу үшін *Қосымша* түймесін басыңыз;
2) *Аудит* қосымша бетінде *Барлығы* аудит элементін таңдаңыз және *Өзгерту* түймесін басыңыз;
3) Пайда болған терезеде файлдар, папкалар және олардың атрибуттарына қолжетімділікке, сонымен қатар, файлдар мен папкаларды өзгертуге жауап беретін аудит опцияларын таңдаңыз. Аудит опцияларын баптағаннан кейін, ОК түймесін басыңыз. Аудиттің екі түрі бар:
   - *сәттілік* —аудит ақпараты жазбасы қадағаланатын әрекеттің сәтті орындалуы кезінде жүзеге асады;
   - *қабылдамау* — аудит ақпараты жазбасы қадағаланатын әрекеттің сәтсіз орындалуы кезінде жүзеге асады;
4) жалпы папка баптауларын аяқтау үшін алдында ашылған барлық терезелер мен қосымша беттердегі өзгерістерді растау қажет.

5.23. Сурет. Дерекқорды қалпына келтіру терезесі



5.6-сурет. Топтық саясаттың құрылған нысанының аудит саясаты

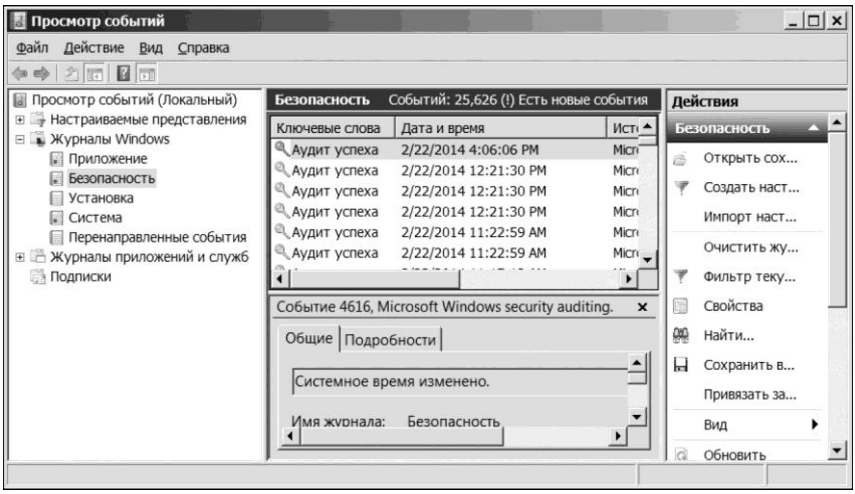
Аудит саясатын баптау. Топтық саясат нысанын құру және оны ол үшін жалпы ресурстардың аудиті жүргізілетін доменмен байланыстыру қажет болсын. Топтық саясат нысандарын құру және оларды байланыстыру 3.4-бөлімшеде қарастырылған.

Құрылған топтық саясат нысаның баптау үшін келесі әрекеттерді орындау қажет:

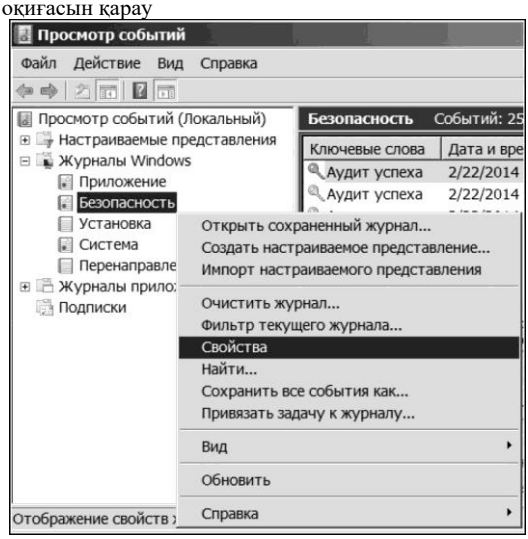
1) «Топтық саясаттарды басқару» жабдықтамасында құрылған топтық саясат нысанын белгілеңіз және мәнмәтін мәзірі көмегімен *Өзгерту* командасын таңдаңыз*;*
2) *Пайда болған Топтық саясаттарды басқару редакторы* терезеде Компьютер конфигурациясы/Саясаты/ Windows конфигурациясы/Қауіпсіздік параметрлер/Жергілікті саясаттар/Аудит саясаты торабын ашыңыз және аудиттің қолжетімді саясаты терезесінен Нысандарға қолжетімділік аудиті элементін ашыңыз (5.6-сурет)*;*
3) *Пайда болған Қасиеттер терезесінде:* Нысандарға қолжетімділік аудитінен Келесі саясат параметрлерін анықтау, Сәттілік және Қабылдамау опцияларын таңдаңыз және ОК түймесін басыңыз.

Жалпы ресурстар аудитімен байланысты оқиғаларды қадағалауды «Оқиғаларды көріп шығу» бағдарламасынан көруге болады. Аудит оқиғаларын қарау үшін Windows журналдары/Қауіпсіздік торабын таңдау қажет (5.7-сурет). Қажет болған жағдайда, журналдың ең үлкен көлемі және журналды тазарту әдісі секілді журналды жүргізу параметрлерін баптауға болады. Журнализацияның қасиеттерін баптау үшін бапталатын журналға арналған мәнмәтін мәзірі көмегімен Қасиеттер командасын таңдаңыз (5.8-сурет).

Пайдаланушылардың ресурстарға қолжетімділік құқығын баптау. Пайдаланушылар мен топтардың есеп жазбалары файлдық сервер ресурстарына икемді қолжетімділікті қамтамасыз етіді.



5.7-сурет. Аудит оқиғасын қарау



Жалпы ресурсқа рұқсат бір-біріне тәуелді емес екі деңгейде анықталады: жергілікті NTFS рұқсаттарымен; жалпы ресурсқа (Windows үшін SMB және Linux үшін NFS) қолжетімділік үшін қолданылатын хаттамалармен.

Деңгейлер бір-біріне тәуелсіз болғандықтан қолжетімділік құқығын анықтау кезінде ең қатаң шектеу қолданылады.

SMB хаттамасы жүйеде белгіленген пайдаланушылар мен топтар негізінде қолжетімділік құқықтарын үлестіруді қамтамасыз етеді. NFS хаттамасы клиенттік компьютерлер мен топтардың желілік атаулары арқылы қолжетімділікті басқарады.

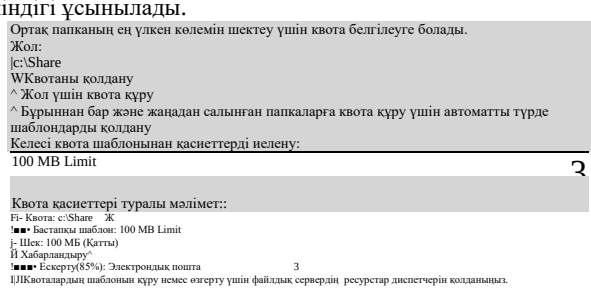
Жалпы ресурс рұқсаттарын баптау түрлі әдістермен жүзеге асырылады. Ары қарай «Жалпы ресурстар мен сақтау орны» *(Іске қосу/Әкімшілендіру/Жалпы ресурстар мен сақтау орындарын басқару)* бағдарламасында қолжетімді жалпы

5.23. Сурет. Дерекқорды қалпына келтіру терезесі

папкаларды дайындау шебері көмегімен жалпы ресурсты қосу әдісі қарастырылады.

Жалпы папкаларды дайындау шебері көмегімен жалпы ресурсты қосу үшін келесі әрекеттерді орындау қажет:

1) *Әрекеттер/Жалпы ресурсты дайындау* панелінен қолжетімді жалпы папкаларды дайындау шеберін ашу немесе *Әрекеттер/Жалпы ресурсты дайындау* мәзір тармағын таңдау қажет;
2) Шебердің бірінші парақшасында ортақ етілетін ресурсты көрсету қажет;
3) Егер, NTFS рұқсаттарын өзгерту қажет болса Ия элементін таңдау, NTFS *рұқсатын өзгерту* және *Рұқсаттарды өзгерту* түймесін басу қажет; NTFSрұқсаттарын баптау кезінде жүйеде белгіленген түрлі пайдаланушылар мен топтарға қолжетімділік опциясын баптауға рұқсат беретін терезе ашылады;
4) Шебердің келесі кезеңінде қолжетімділік хаттамасы мен ресурс атауын енгізу қажет;
5) Келесі парақшада *Қосымша* түймесі көмегімен қолжетімділік хаттамасының қосымша параметрлерін баптау қажет;
6) Келесі парақшада қолжетімділік хаттамасы рұқсаттарын баптау қажет. Егер, пайдаланушылар мен топтардың ерекше рұқсаттары үшін элемент таңдалса, *Рұқсаттар* түймесі арқылы рұқсаттардың икемді баптауы қолжетімді болады;
7) Шебердің келесі қадамында бапталатын ресурс үшін (5.9-сурет) квоталарды қосу және баптау қажет. Квоталарды құрастыру шаблонын таңдау мүмкіндігі ұсынылады.



5.9-сурет. Квоталарды баптау

Шаблондарды басқару Файлдық сервердің ресурстар диспетчері құрауышы арқылы қолжетімді;

8) Файлдарды бұғаттау фильтрін қолдану және таңдау. Бұл жағдайда файлдарды бұғаттау фильтрлері файлдық сервердің ресурстар диспетчерінде бапталады. Windows операциялық жүйесі пайдаланушыға пайдаланушылармен кеңейтілуі мүмкін стандартты фильтрлер жинағын ұсынады;

9) Келесі қадамда DFS (DFS— үлестірілген файлдық жүйе) атаулар кеңістігінде ортақ ресурсты жариялау туралы сұраққа жауап беру;
10) Ақырғы кезеңде құрылатын ортақ ресурс параметрлерімен танысып, оны құру үшін *Құру* түймесін басу қажет.

WindowsServer2008 R2-дегі файл-сервеврдің ресурстар диспетчері *Іске қосу/Әкімшілендіру/Файлдық сервердің ресурстар диспетчері* мәзір тармағы арқылы қолжетімді.

Файлдық сервердің ресурстар диспетчері келесі тапсырмаларды орындау үшін тағайындалған:

- Сервер ресурстарына арналған квоталар мен квота шаблондарын басқару;
- Файлдарды бұғаттау фильтрлері мен оның шаблондарын басқару;
- Файлдық сервердің ресурстарына бақылау жүргізу;
- Файлдық сервердің ресурстарын пайдалану туралы есептіліктерді генерациялау және т.б.

5.3.

ПОШТАЛЫҚ СЕРВЕРДІ СҮЙЕМЕЛДЕУ ЖӘНЕ БАҚЫЛАУ

Пошталық сервер, немесе *поштаны қайта жолдау агенті*, — келесі қызметтерді жүзеге асыратын электрондық поштаны жеткізу құралы:

- Жіберушілерден хаттарды қабылдау;
- Алушыларға хаттарды жеткізу;
- Хатты жіберушіден сәтті қабылдау және алушыға хатты сәтті жеткізу арасындағы уақыт аралығында хаттарды сақтау.

Пошталық сервер мен оның сүйемелдеуін конфигурациялау кезінде электрондық хат алмасу кезінде туындайтын спам-фильтрлерді пайдаланумен, алушылар сервері тарабында жіберілетін хаттардың ауытқуымен, зиян келтіретін нысандарды іздеу мақсатындағы салуларды талдау және тағы басқа қиындықтармен байланысты бірқатар қиындықтар туындайды.

Поштаны жіберу және қабылдауды бақылау. Әдетте, поштаны жіберуді бақылау келесі қызметтерден тұрады: жіберілетін ақпаратты бақылау; жіберілетін ақпаратты алушылардың мекенжайлары аудиті.

Егер, корпоративтік пошталық серверді пайдалануды қарастырсақ, алушылардың мекенжайлары аудиті көбіне ActiveDirectory нысандарында негізделген жіберілім тізімдерімен байланысты. Мұндай жағдайда, пошталық сервер пайдаланушыларымен сыртқы желіге жіберілетін ақпаратты қадағалау қажет.

Жіберілетін ақпаратты бақылау келесі әдістермен орындалуы мүмкін:

- *Егер, пайдаланушының қатысуынсыз жіберілетін контентті қадағалау механизмдері пайланатын болса, автоматтық түрде. Жіберуді қабылдамау ережелері пошталық сервер әкімшісімен бапталады және әрбір нақты жағдайда бұл ережелер әртүрлі*;
- *Модератордың қатысуымен, оның міндеті жіберілетін ақпаратты талдау және оны жіберуге немесе жібермеуге шешім жасау.*

Ары қарай MicrosoftExchangeServer2010 шешімі үлгісінде шығыс поштасын моджерациялау механизмі қарастырылады.

MicrosoftExchangeServer2010-дегі модерациялау механизмі пайдаланушымен хатты жіберу және жіберілетін хатты пошталық сервердің жіберу кезегіне жіберу арасындағы аралық инстанциямен ерекшеленеді. Модерациялау кезеңінде жіберілетін пошта модераторы хатты жіберу немесе жолдамау туралы шешім қабылдайды. Хат жолданбаған жағдайда жиінде жолданбау себебі туралы хабар береді.

Модерацияны қолдану кезінде хат келесі тізбектен өтеді:

- Хатты құру;
- Хатты алушыға жолдау (немесе жіберілім тізімі арқылы жолдау;
- Егер, модерациялау ережесі іске қосылса, хатты модерациялау кезегіне

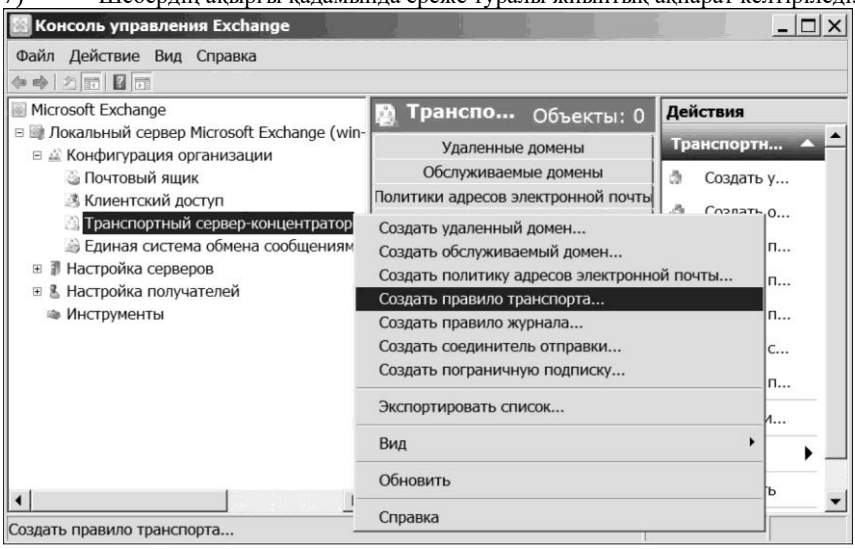
жолдау;

- Модераторды хатты жолдау туралы шешім қабылдау үшін хабарландыру;
- Модератормен хатты жолдау немесе жолдамау туралы шешім қабылады;
- Егер, хат модератормен қабылданған болса, хатты жолдау кезегіне жіберу;
- Олай болмаған жағдайда, хатты жою және бұл жайында жіберушіні хабарлау.

MicrosoftExchangeServer2010-да модерациялауды баптау.

Модерациялауды баптау үшін келесі әрекеттерді орындау қажет:

1) Іске қосу/Барлық бағдарламалар/Microsoft Exchange Server 2010/ Exchange Management Console мәзір тармағы көмегімен *Exchange басқару консолін ашу*;
2) *Мекеме конфигурациясы/Көліктік шоғырлауыш сервер торабын ашамыз және мәнмәтін мәзірі көмегімен Көлік ережесін құру командасын таңдаймыз (5.10-сурет);*
3) Ашылған жаңа көлік ережесін құру шеберінің бастапқы парақшасында ереже атауын береміз және *Ары қарай* түймесін басамыз;
4) Шартты таңдай отырып, *2-қадам* (қажет болған жағдайда) терезесінде ереже сипаттамасын өзгертеміз және *Ары қарай* түймесін басамыз. Мысалы, егер, *Келесі жіберушілерден хаттар* шарты қолданылатын болса, сипаттаманы өзгерту терезесінде хаттары модерациялауды талап ететін жіберушілер мекенжайларын енгізуге болады;
5) *Әрекеттер* парақшасында ереже іске қосылған уақытта орындалатын әрекеттерді көрсету қажет;
6) Шебердің келесі қадамында ереже үшін артықшылықтарды таңдау;
7) Шебердің ақырғы қадамында ереже туралы жиынтық ақпарат келтіріледі.

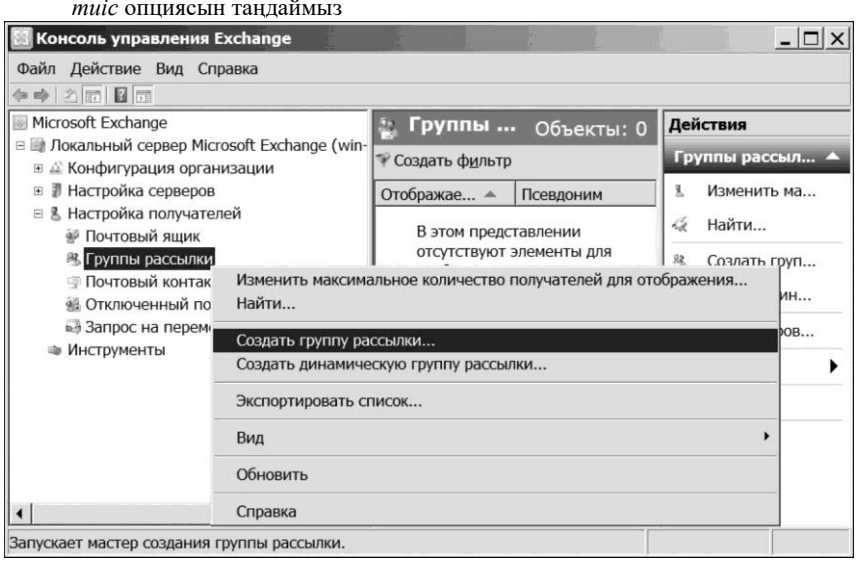


5.10-сурет. Exchange басқару панелі

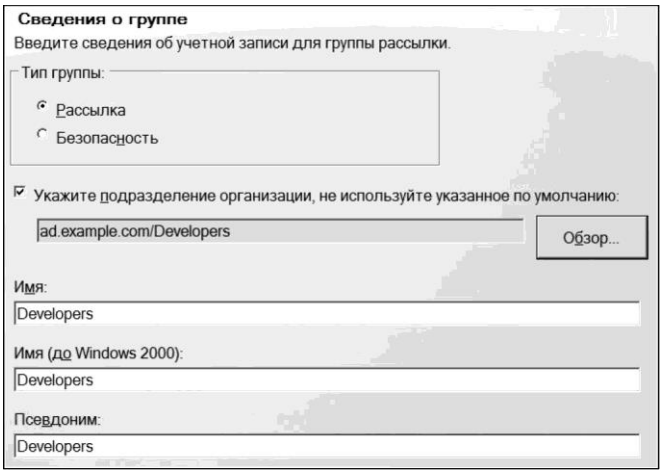
Шебердің жұмысын аяқтау үшін Құру түймесін басамыз.

Жіберілім тізіміне арналған модерацияны баптау келесі әрекеттерден құралады:

1) Іске қосу/Барлық бағдарламалар/Microsoft Exchange Server 2010/ Exchange Management Console мәзір тармағы көмегімен *Exchange басқару консолін ашу*;
2) *Алушыларды баптау/Жіберілім тобы торабын ашамыз және мәнмәтін мәзірі көмегімен Жіберілім тобын құру командасын таңдаймыз (5.11-сурет);*
3) Пайда болған жаңа жіберілім тобын құру шеберінде бұрыннан бар топты немесе *Жаңа топ* командасын таңдаймыз және *Ары қарай* түймесін басамыз*;*
4) Шебердің келесі кезеңінде топ түрін, топ атауын көрсетеміз, одан соң, *Ары қарай* түймесін басамыз (5.12-сурет);
5) Жаңа жіберілім тобын құру шеберінің ақырғы кезеңінде *Құру* түймесін басамыз;
6) Келесі кезеңде бапталатын жіберілім тобын белгілейміз және мәнмәтін мәзірі көмегімен *Қасиеттер* командасын таңдаймыз;
7) Топ қасиеттері терезесінде *Пошта ағыны параметрі* қосымша бетін ашамыз және Х*аттарды басқару* командасын таңдай отырып, *Қасиеттер* түймесін басамыз*;*
8) Ашылған терезеде *Осы топқа жіберілген хаттар модераторымен бекітілуі тиіс* опциясын таңдаймыз



5.11-сурет. Exchange басқару консолінің Жіберілімдер тобы торабы



5.12-сурет. Құрылып жатқан жіберілім тобы мәліметтерін көрсету \

Хаттарды жолдау модерацияны талап етпейтін топтардың, жіберушілердің модераторын көрсетуге, сонымен қатар, хаттары жолданбаған жағдайда жіберушілерді хабарлау әдісін көрсетуге болады (5.13-сурет).

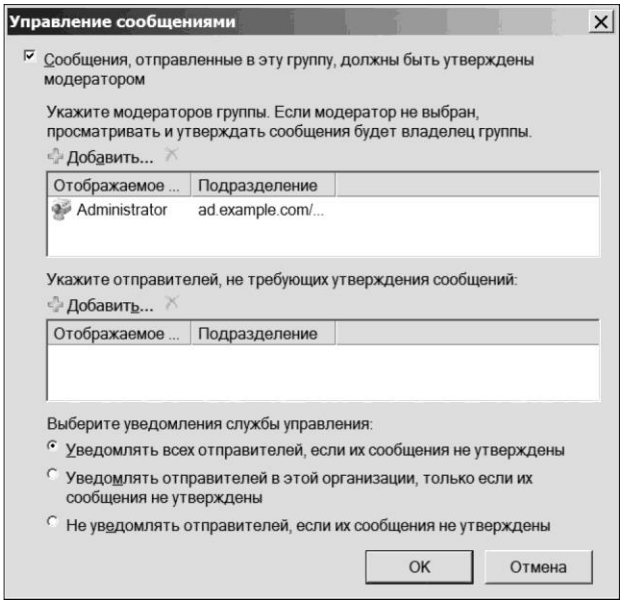
Пошталық аккаунттарға пайдаланушылардың қолжетімділік құқығын баптау.

Microsoft Exchange Server 2010 бағдарламасы Active Directory-мен біріктірілген. Бір ExchangeServer2010 ұймы ActiveDirectory бір орманымен байланысты.

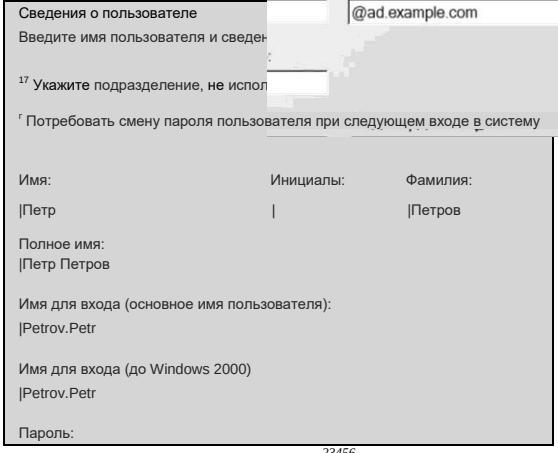
MicrosoftExchangeServer2010 бағдарламасында алушылардың бірнеше түрі бар. Алушылардың ең жиі таралған түрі пошталық жәшік болып табылады, себебі, пошталық жәшік ActiveDirectory пайдаланушысының есептік жазбасымен байланысты және хат алмасудың негізгі құралы болып табылады. MicrosoftExchangeServer2010 бағдарламасында пошталық жәшіктер неше түрлі түрде болып келеді, ары қарай пайдаланушылардың пошталық жәшіктерін қарастырайық.

Пайдаланушының пошталық жәшігін құру үшін келесі әрекеттерді орындау қажет:

1) Іске қосу/Барлық бағдарламалар/Microsoft Exchange Server 2010/ Exchange Management Console мәзір тармағы көмегімен *Exchange басқару консолін ашу*;



5.13-сурет. Топтық жіберілім модерациясын қосу



5.14-сурет. *Пайдаланушы туралы мәліметтер*[23456] парақшасы

---

2 Алушыларды баптау торабын белгілеп, және мәнмәтін мәзірі көмегімен *Пошталық жәшік құру* командасын басыңыз;

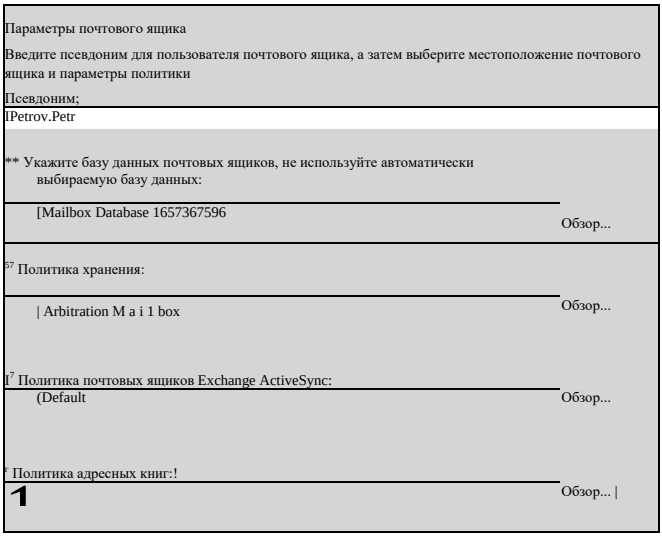
3 Шебер парақшасында *Пайдаланушының пошталық жәшігі* элементін таңдаңыз және *Ары қарай* түймесін басыңыз;

4 Бұрыннан келе жатқан ActiveDirectory каталогтар қызметі пайдаланушысын таңдаңыз немесе жаңа пайдаланушыны құрыңыз;

5 Егер, алдыңғы қадамда *Жаңа пайдаланушы* тармағы таңдалған болса, *Пайдаланушы туралы мәліметтер* парақшасы ашылады. Құрылып жатқан пайдаланушы туралы мәліметті толтырыңыз (5.14-сурет). бұл парақтың жолдары ActiveDirectory каталогтар қызметі пайдаланушыларының есептік жазбаларын құру кезіндегі жолдарға ұқсас (3.3-бөлімшені қараңыз). *Шолу* түймесі көмегімен бұрыннан бар ActiveDirectory бөлімшесін таңдауға болады;

6 Шебердің келесі парақшасында пошталық жәшік параметрлерін баптауға болады (5.15-сурет). Бұл парақшада келесі жолдарды толтыру қажет:

- Лақап аты жолы — пайдаланушының мәліметтері негізінде автоматты түрде толтырылады;
- Пошталық жәшіктердің мәліметтер базасы жолы — егер, оны жалаушаны басу арқылы іске қосса, *Шолу* түймесі көмегімен пошталық жәшіктердің мәліметтер базасын көрсетуге болады;
- Сақтау саясаты жолы — егер, оны жалаушаны басу арқылы іске қосса, *Шолу* түймесі көмегімен пошталық жәшіктерге сақтау саясатын белгілеуге болады;
- *ExchangeActiveSync пошталық жәшіктер саясаты жолы* — егер, оны жалаушаны басу арқылы іске қосса, *Шолу* түймесі көмегімен электрондық поштаға ұялы құрылғылар арқылы қолжетімділікті тағайындауға арналған ExchangeActiveSync саясатын белгілеуге болады;
- Мекенжайлық кітәптар саясаты жолы — егер, оны жалаушаны басу арқылы іске қосса, *Шолу* түймесі көмегімен пошталық жәшіктердің мекенжайлық кітәптар саясатын белгілеуге болады;



5.15-сурет. Пошталық жәшік параметрлері парақшасы

■ *қашықтықта орналасқан мұрағат құру* — егер, мұрағатты бұлтта сақтау талап етілсе. Мұрағаттаудың осы үлгісі Exchange Online баптауын қажет етеді;

8) Шебер жұмысының келесі кезеңінде құрылып жатқан пошталық жәшік туралы жиынтық ақпаратпен танысып, пайдаланушының пошталық жәшігін құру үшін *Құру* түймесін басу қажет;

9) Одан кейін *Аяқтау командасын басу қажет*.

Бұрыннан келе жатқан пошталық жәшіктерді редакциялау үшін келесі әрекеттерді орындау қажет:

- ExchangeActiveSync саясатын белгілеуге болады;
- Мекенжайлық кітәптар саясаты жолы — егер, оны жалаушаны басу арқылы іске қосса, *Шолу* түймесі көмегімен пошталық жәшіктердің мекенжайлық кітәптар саясатын белгілеуге болады;

6 Шебердің келесі қадамында мұрағат параметрлерін баптау қажет.
Мұрағаттаудың келесі үлгілері болуы мүмкін:

- *Мұрағат құрмау* — егер, осы пошталық жәшік үшін мұрағат құру қажет болмаса;
- *Жергілікті мұрағат құру* — егер, пошталық жәшіктің жергілікті мұрағатын құру қажет болмаса. Егер, мұрағаттың осы нұсқасы таңдалған болса, *Шолу* түймесі арқылы пошталық жәшіктің мәліметтер базасын көрсетуге болады;

1) Іске қосу/Барлық бағдарламалар/Microsoft Exchange Server 2010/ Exchange Management Console мәзір тармағы көмегімен *Exchange басқару консолін ашу;*

2) *Алушыларды баптау* торабын ашыңыз және нәтижелер терезесінде пайдаланушының өзгертілуге тиіс пошталық жәшігін таңдаңыз;

3) Мәнмәтін мәзірі көмегімен таңдалған пошталық жәшік үшін *Қасиеттер* командасын таңдаңыз.

Пайдаланушылардың пошталық жәшіктеріне қолжетімділік құқығын басқару Exchange (ExchangeManagementConsole) басқару консолімен де, Exchange (ExchangeManagementShell) командалық консолімен де жүзеге асыруға болады.

Exchange пошталық жәшігіне толық құқық беру үшін Exchange басқару консолі құралдарымен келесі әрекеттерді орындау қажет:

1) Іске қосу/Барлық бағдарламалар/Microsoft Exchange Server 2010/ Exchange Management Console мәзір тармағы көмегімен *Exchange басқару консолін ашу;*
2) *Алушыларды баптау* торабын ашыңыз және нәтижелер терезесінде пайдаланушының өзгертілуге тиіс пошталық жәшігін таңдаңыз;
3) Мәнмәтін мәзірі көмегімен таңдалған пошталық жәшік үшін *Толық қолжетімділікке рұқсатты басқару* командасын таңдаңыз.
4) Пайда болған терезеде осы пошталық жәшікке толық қолжетімділікке ие болатын пайдаланушыны қосу үшін *Қосу* түймесін басыңыз;
5) Қолжетімді топтар мен ActiveDirectory каталогтар қызметін пайдаланушылар тізімі шығады. Оның ішінен бапталық жатқан пошталық жәшікке толық қолжетімділік тағайындалған пайдаланушылар мен топтарды таңдау қажет;
6) Шебердің ақырғы жұмыс кезеңінде пайдаланушылар мен топтарды қосқаннан кейін *Басқару* түймесін басыңыз.

Exchange командалық консолынің көмегімен пошталық жәшікке толық қолжетімділік рұқсатын орнату үшін келесі әрекеттерді орындау керек:

1) Іске қосу/Барлық бағдарламалар/Microsoft Exchange Server 2010/ Exchange Management Console мәзір тармағының көмегімен *Exchange командалық консолін ашу керек;*
2) команданы енгізу және «Енгізу» басу керек:

```
Add-MailboxPermission -identity Petrov.Petr -accessrights:fullaccess -user "Domain Users"
```

Параметр — *identity* пошталық жәшіктік сәйкестендіруші үшін жауап береді, ал — *user* қолжетімділікке толық құқық берілетін пайдаланушы немесе топ үшін жауап береді. Параметр — *accessrights:fullaccess* болса *DomainUsers* тобында пошталық жәшікке толық қолжетімділік берілетінін көрсетеді.

Толық қолжетімділікті жою үшін келесі команданы қолдану керек:

```
Remove-MailboxPermission -identity Petrov.Petr -accessrights:fullaccess -user "Domain Users"
```

5.4. SQL-СЕРВЕРДІ СҮЙЕМЕЛДЕУ ЖӘНЕ БАҚЫЛАУ

Сервер конфигурациясын бақылау. SQL-сервер конфигурациясының аудиті MicrosoftSQLServer2008 R2 МББЖ үлгісінде қарастырылатын болады.

SQLServer конфигурациясын бақылау MicrosoftSQL-Server МББЖ-да болып жатқан оқиғаларды қадағалау мен журналдауды қарастырады. SQLServer2008 Enterprise-те SQLServer аудит шағын жүйесінің көмегімен автоматты аудит жүргізу мүмкіндігі бар. Сол сияқты, MicrosoftSQL-Server үшін шеттегі өндірушілерден осы мәлесені шешу жолдары бар.

SQLServer-де конфигурацияны бақылау келесі деңгейлерде қамтамасыз етілуі мүмкін: SQLServer барлық данасы үшін; SQL-сервердің жеке мәліметтер базасы үшін.

Сервер данасы деңгейіндегі конфигурацияны бақылау жағдайында сервер деігейінің әрекеттеріне жауап қайтаратын аудиттің жалғыз нысанын ғана құруға болады. Жеке мәліметтер базасын бақылау деңгейінде, сондай-ақ, әрбір мәліметтер базасы үшін аудиттің бір ғана сипаттізімі қарастырылады.

SQLServer аудитінің шағын жүйесі оқиғалар тобын немесе жеке оқиғаларды қадағалауды қарастырады.

Конфигурация бақылауының бақыланатын оқиғаларын үш топқа бөлуге болады:

1) сервер деңгейінің оқиғалары (сервердің жаһандық оқиғалары);
2) мәліметтер базасы деңгейінің оқиғалары (өңдеу тілдері мен мәліметтерді сипаттау операциялары);
3) аудит деңгейінің оқиғалары (аудит кезінде орын алатындар).

Аудит нәтижелері келесі әдістердің бірімен бекітілуі мүмкін:

- тағайындау файлындағы жазба;
- Windows қауіпсіздігінің оқиғалар журналындағы жазба;
  - Windows қосымшаларының оқиғалар журналындағы жазба (алдыңғыға қарағандай қауіпсіздігі төмен, себебі, қосымшалар оқиғаларының журналына қолжетімділікті аутентификациядан өткен кез-келген пайдаланушы алу мүмкін).

Windows оқиғалар журналын көру үшін оқиғаларды көру бағдарламасын қолдануға болады (WindowsServer2008 R2 үшін орналасуы: *Іске қосу/Әкімшіліктендіру/Оқиғаларды көру).* Тағайындау файлдарын *Журналды көру құралы* арқылы ашуға болады (SQLServer-де).

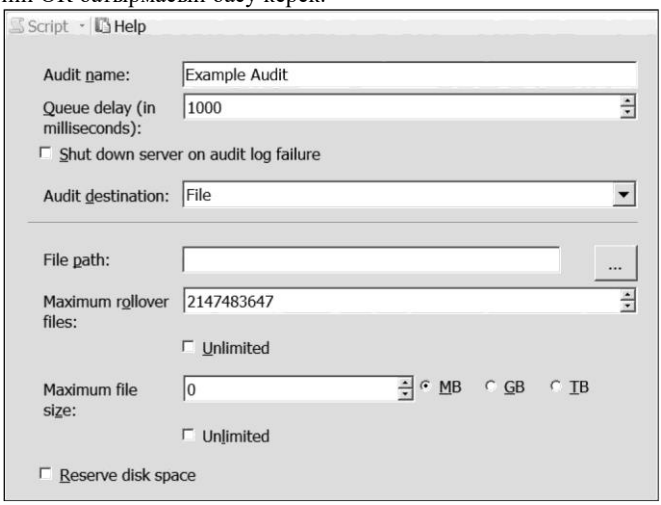
Аудиттің жаңа сипаттамасын құру. Сервер немесе мәліметтер базасының аудиті сипаттамасын құру алдында аудиттің жаңа сипаттамасының нысанын құру керек.

Для создания новой спецификации аудита в SQLServer2008 R2-де аудиттің жаңа сипаттамасын құру үшін келесі әрекетерді орындау керек:

1) *SQL Server Management Studio ортасын ашу керек* (Іске қосу/Барлық

бағдарламалар/Microsoft SQL Server 2008 R2/SQL Server Management Studio);

2) *ObjectExplorer* панелінде мына торапты <*Сервер атауы* >/*Security/Audits* ашып, мәнмәтін мәзірінің көмегімен *NewAudit* командасын таңдау керек;
3) *CreateAudit* ашылған терезесіне келесі ақпаратты енгізу керек: *Auditname*— аудит атауы, *Auditdestination* — аудит оқиғалары жазбасының әдісі (мақсатты файлы немесе оқиғалар журналы) (5.16-сурет). Егер, *(File)* файлға жазба таңдалса, онда мынаны көрсету керек: *Filepath* — файлға апарар жол және файлдың максималды көлемінің параметрлері. Егер, журнал тармақтарының бірі таңдалса *(Securitylog* немесе *Applicationlog)*, онда SQLServer құралдарымен оларды баптау қажет болмайды;
4) құрылатын аудит сипаттамасының барлық параметрлерін баптағаннан кейін ОК батырмасын басу керек.



5.16-сурет. Аудиттің жаңа сипаттамасының параметрлері

Сервер деңгейінде аудит сипаттамасын құру. Сервер деңгейінде аудит сипаттамасын құру үшін келесі әрекеттерді орындау керек:

1) *SQL Server Management Studio ортасын ашу керек* (Іске қосу/Барлық бағдарламалар/Microsoft SQL Server 2008 R2/SQL Server Management Studio);
2) «Object Explorer» панелінде <*Имясервера*>/ *Security/Server Audit Specifications* торабын ашу және мәнмәтіндік мәзірдің көмегімен *New Server Audit Specification* командасын таңдау керек. Сервер деңгейіндегі аудит сипаттамасы параметрлерінің терезесі ашылады *CreateServerAuditSpecification* (5.17-сурет). *Name* жолы сервер деңгейіндегі сипаттама атауына жауап береді, *Audit* жолы — аудит сипаттамасының

таңдауы үшін жауап береді (бұған дейін ExampleAudit сипаттамасы құрылған). Төменде оның көмегімен сервер деңгейінің қадағаланатын оқиғаларын қосу жүзеге асырылатын аудит әрекеттерінің кестесі орналасқан (бұл жағдайда сәтсіз кіру мен құпиясөзді ауыстыру оқиғалары таңдалған);

3) Аудит параметрлерінің баптауларынан кейін ОК батырмасын басу арқылы сипаттаманы сақтау керек;

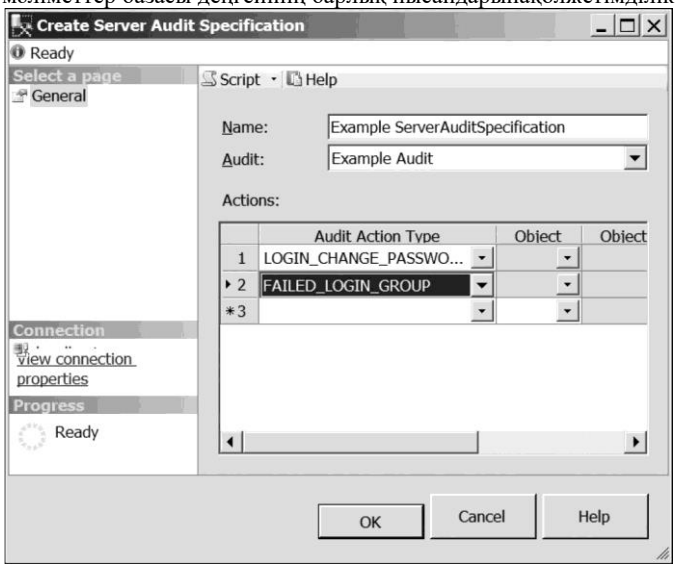
4) құрылған сипаттаманы қосу үшін *Audits* торабын кеңейтіп, құрылған сипаттаманы ерекшелеп, мәтінмәндік мәзірдің көмегімен *EnableAudit* командасын таңдау керек.

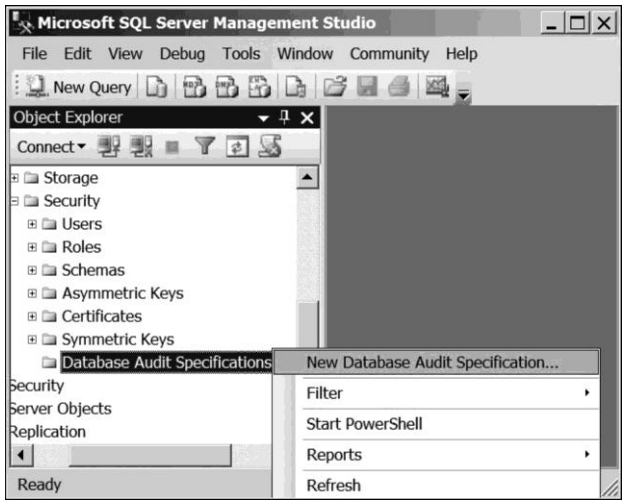
5) *Мәліметтер базасы деңгейінде аудит сипаттамасын құру.* Мәліметтер базасы деңгейінде аудит сипаттамасын құру үшін келесі әрекеттерді орындау керек:

1) *SQL Server Management Studio ортасын ашу керек* (Іске қосу/Барлық бағдарламалар/Microsoft SQL Server 2008 R2/SQL Server Management Studio);

2) *«Object Explorer» панеліндегі* <Сервер атауы>/ <Мәліметтер базасының атауы>/Security/Database Audit Specifications торабын ашу керек және *мәнмәтіндік мәзірдің көмегімен* New Database Audit Specification командасын таңдау керек *(5.18-сурет);*

3) *CreateDatabaseAuditSpecification* ашылған терезесінде аудит оқиғаларын күйге келтіру керек (5.19-сурет). *Name* жолы аудит сипаттамасының атауы үшін, *Audit* жолы — аудит сипаттамасын таңдау үшін жауап береді (бұл жағдайда DBAudit алдын ала құрылған сипаттамасы таңдалған). Төменде оның көмегімен мәліметтер базасы деңгейінің қадағаланатын оқиғаларын қосу жүзеге асырылатын аудит әрекеттерінің кестесі орналасқан. *AuditActionType* атрибуты аудиттің оқиғалар түріну жауап береді. *ObjectClass* атрибуты бақыланатын нысан түрін көрсетуге мүмкіндік береді, мысалы, әліметтер базасын *(Database)* немесе кестені *(Table). Object Class* атрибуты қолжетімді тізімнен таңдауға болатын нысан атауына жауап береді (таңдау үшін шолу батырмасын басу керек «...», ал пайда болған диалог терезесінде *Browse* батырмасының көмегімен мәліметтер базасы деңгейінің барлық нысандарынақолжетімділік алу);





5.18-сурет. Мәліметтер юазасы деңгейінде аудит сипаттамасын құру

PrincipalName атрибуты нысан таңдау ұқсастығы бойынша қолжетімді тізімнен таңдауға болатын аудит субъектіінің атауы үшін жауап береді;

4) сипаттаманың барлық қажетті параметрлерін орнатқаннан кейін, өзгерістерді сақтау үшін OK батырмасын басыңыз;

5) құрылған спецификацияны қосу үшін *Audits* торабын ашып, құрылған сипаттаманы ерекшелеу керек және мәнмәтіндік мәзірдің көмегімен *EnableAudit* командасын таңдау керек.

Мәліметтер базасын резервтік көшірмелеу және қалпына келтіру. Мәліметтер базасын сақтық көшірмелеу және қалпына келтіру мәліметтер базасын басқарудағы ең маңызды процестердің бірі болып табылады. Бұл сақталған деректерді келісілген күйінде сақтауға мүмкіндік беретін механизм, себебі оның құзыретті конфигурациясы болған жағдайда, жүйенің кейбір күтпеген қателерінен кейін мәліметтер базасын қалпына келтіру мәселесін шешеді. Жүйенің ақауы ретінде сақталған ақпараттың тұтастығының бұзылуына алып келетін кез-келген оқиғаны түсінуге болады. Ақау себептері мыналар:

- пайдаланушылар қатесі;
- жабдықтың ақауы (тасымалдағыштардың сынуы, электр қуатының проблемалары және аппараттық сипаттағы басқа да себептер);
- мәліметтердің келісілуін қолдау құралдарымен байланысты әзірлеушілердің қатесі.

Бұдан әрі қлпына келтірудің қарапайым моделін қолданатын MicrosoftSQLServer2008 резервтік көшірмелеу механищмдері қарастырылатын болады.

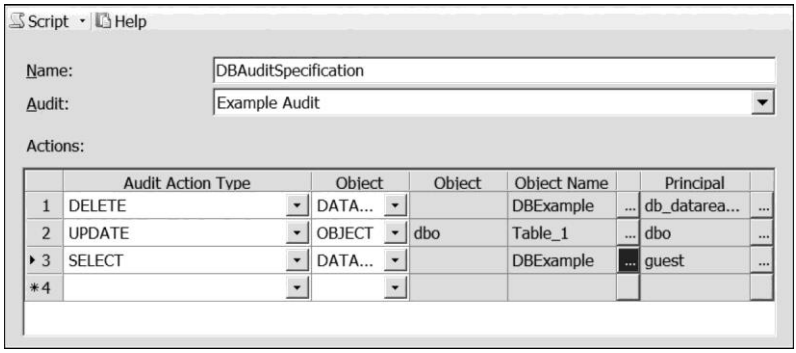
Қарапайым қалпына келтіру үлгісі мәліметтер базасының резервтік көшірмесін

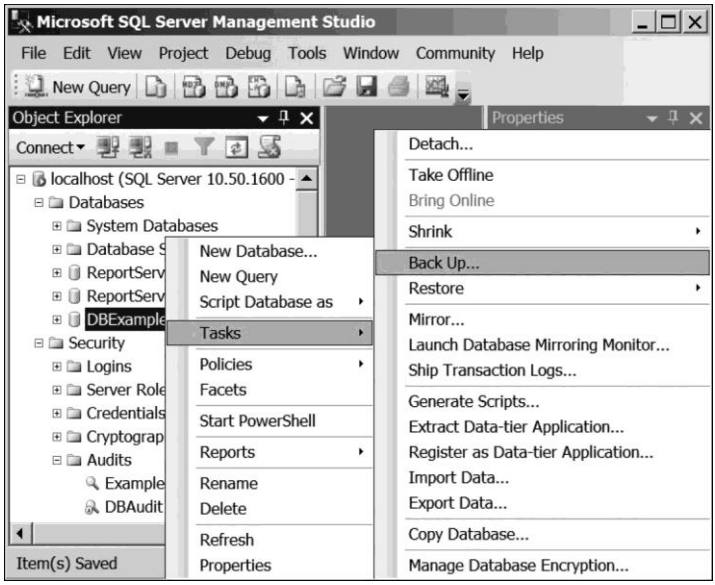
және файлдардың резервтік көшірмелерін сүйемелдейді, бірақ ол журналдардың резервтік көшірмесін қолдамайды, бұл өз кезегінде резервтік көшірмелеу және қалпына келтіру процесін айтарлықтай жеңілдетеді. Қарапайым модельдің кешілігі – мәліметтерді соңғы резервтік көшірмелеу күйіне дейін ғана мәліметтер базасын қалпына клетіру қарастырылуында. Соңғы өзгерістерді жоғалту сыни болып табылатын жүйелерде резервтік көшірмелеудің бұл жолы қолайсыз болады және сол себепті толық қалпына келтіруге арналған модель қолданылады.

SQLServer2008 R2-де Қалпына келтірудің қарапайым үлгісін пайдалану арқылы резервтік көшірменің екі нұсқасы қарастырылған: мәліметтер базасының толық резервтік көшірмесі; мәліметтер базасының қатысты резервтік көшірмесі.

Резервтік көшірме құру. Резервтік көшірме құру келесі әрекеттерді орындау керек:

1) *SQL Server Management Studio ортасын ашу керек* (Іске қосу/Барлық бағдарламалар/Microsoft SQL Server 2008 R2/SQL Server Management Studio);
2) *ObjectExplorer* панелінде <Сервер атауы>/ <Мәліметтер базасының атауы> торабын ерекшелеп, мәнмәтіндік мәзірдің көмегімен Tasks/BackUp командасын таңдау керек (5.20-сурет);
3) Мәліметтер базасын резервтік көшірмелеудің ашылған терезесінде *Source (Көзі)*жолында *Data base* жолында мәліметтер базасын көрсету керек.





5.20-сурет. Пайдаланушылардың мәліметтер базасының резервтік көшірмесін құру

Резервтік көшірмелеу түрі толық резервтік көшірмелеуді *(Full),* қатынасты (*Differential*) немесе транзакциялар*(Transactionlog)* журналының көшірмелеуін көрсетете алады. Тек көшірмелеуге арналған резервтік көшірмелеу опциясы *(Copy-onlyBackUp)* одан әрі қалпына келтіру тізбегінде қолданылмайтын тек мәліметтер базасын көшірмелеуге арнағлған резервтік көшірмелеу құруға мүмкіндік береді;

4) *Мәліметтердің резервтік жинағы (BackUpSet)* аймағының параметрлерін баптау. *Name* өрісі мәліметтердің резервтік жинағының атына жауап береді. Кейінгі өріс *After* резервтік деректер жиынтығының жарамдылық мерзімін көрсетуге мүмкіндік береді. *On* өрісі резервтік деректер жиынының жарамдылық мерзіміне жауап береді;
5) *Destination* тағайындау өрісінде резервтік көшірмелеу тасымалдағыштарының жолын көрсету керек;
6) Резервтік көшірмелеудің барлық параметрлерін күйге келтірген соң OK батырмасын басу керек.

Резервтік көшірме терезесі пайдаланушыға *Options* парақшасында қолжетімді басқа параметрлер жиынтығымен қамтамасыз етеді (5.21-сурет). Мәліметтер базасының резервтік көшірмесін құру кезінде (толық немесе қатысты) осы беттің параметрлері тасымалдағыштың қайта жазылуы мен сенімділдігіне жауап береді.

Тасымалдағышты қайта жазу (Overwrite Media):

1) тасымалдағыштардың жиынтығында резервтік көшірмесін құру:

■ бар резервтік мәліметтер жинағын қосу;

■ мәліметтердің бар барлық резервтік жинақтарын қайта жазу;

2) жаңа тасымалдағыштар жинағына резервтік көшірмені орындау және бар барлық резервтік көшірмелерді жою.

*Checkmediasetnameandbackupsetexpiration*y опциясы тасымалдағыштар жинағы мен мәліметтердің резервтік жинағының тексерілуін көрсетеді.

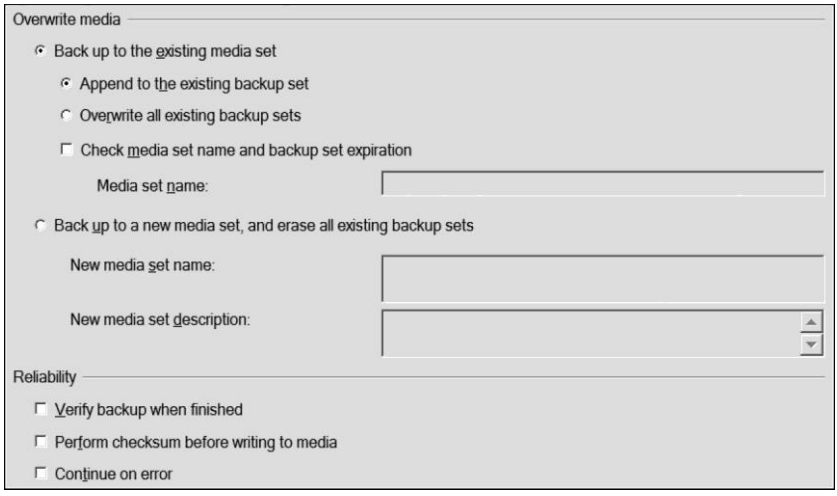
Сенімділік (Reliability):

- аяқталған соң резервтік көшірмелеуді тексеру;
- тасымалдағышқа жазар ақырғы соманың есептеуі;
- соңғы соманың қателігі кезіндегі жалғастыру.

Резервтік көшірмелеуді қалпына келтіру. Резервтік көшірмелеуді қалпына келтіру үшін мына әрекеттерді орындау керек:

1) *SQL Server Management Studio ортасын ашу* (Іске қосу/Барлық бағдарламалар/Microsoft SQL Server 2008 R2/SQL Server Management Studio*);*

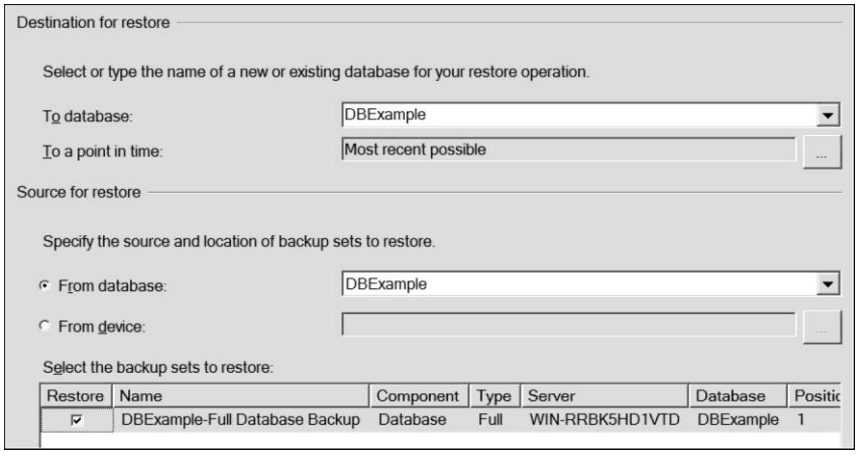
2) *ObjectExplorer панелінде <Сервер атауы >/<Мәліметтер базасының атауы>* торабын ерекшелеп, мәнмәтіндік әмзірдің көмегімен *Tasks/BackUp командасын таңдау керек* (5.22-сурет);



5.21-сурет. Резервтік көшірмелеу терезесінің *Options парақшалары параметрлерінің жинағы*

5.22-сурет. Мәліметтер базасы және резервтік көшірмелеуді қалпына келтіруқ

3) қалпына келтіру параметрлерінің ашылған терезесінде қалпына келтірілетін мәліметтер базасын немесе жаңа мәліметтер базасының атауы көрсету керек (5.23-суретті қараңыз). Toapointintime өрісі қалпына келтіру орындалатын уақыт сәтіне жауап береді. Sourceforrestore қалпына келтіруге арналған жинақтар көзі үшін жауап береді.



4) қалпына келтірудің барлық параметрлерін күйге келтірген соңі ОК батырмасын басу керек.

Қалпына келтіру терезесі пайдаланушыға *Options* бетінде қолжетімді басқа параметрлер жиынтығын, соның ішінде келесі қалпына келтіру опцияларын ұсынады:

- бар мәліметтер базасын қайта жау;
- репликация баптауларын сақтау керек;
- әрбір резервтік көшірмені қалпына келтіру алдында сұраныс жолдау;
- қалпынакелтірілген мәліметтер базасына қолжетімділікті шектеу.

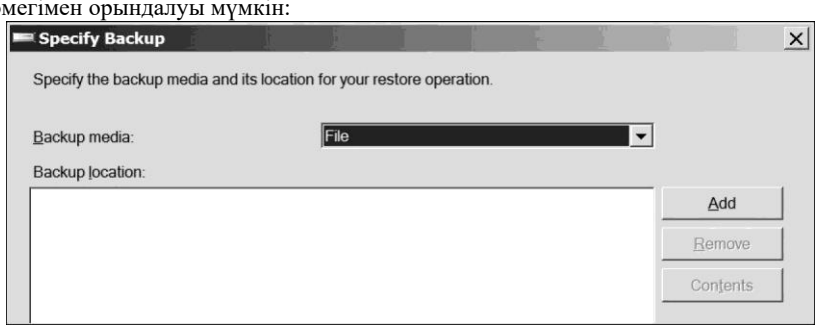
Мәліметтер базасына пайдаланушылардың қолжетімділік құқықтарын баптау. SQLServer2008 R2-де мәліметтер базасына қолжетімділік құқытарын басқару кіру атауын және қорғауды талап ететін нысандарға рөлдерді рұқсат етуді баптаумен орындалады.

SQLServer2008 R2-де мәліметтерге қолжетімділікті басқару субъектілердің түрлі санаттарын қолданумен жүзеге асырылады:

- Windows (мысалы, кіру атауы Windows);
- SQL Server (кіру атауы SQL Server);
- мәліметтер базасы (мәліметтер базасының пайдаланушысы, мәліметтер базасының рөлі, қосымша рөлі).

Қатысушылардың түрлі дәрежелері әрекеттің түрлі аумақтарына ие.

Көрсетілген қатысушылар үшін қолжетімділік құқықтарын басқару мынаның көмегімен орындалуы мүмкін:



- ObjectExplorer графикалық интерфейсі. Бұл қолжетімлілік құқықтарын басқарудың әлдеқайда қарапайым әдісі;
- сақталатын рәсімдер;
- Transact SQL сұраныстары.

Осы әдістердің әрқайсысы қолжетімділік субъектілерінің/объектілерінің мәндерімен және олардың өзара әрекеттерімен көру, өзгерту, құру және басқа да әрекеттерді жасау мүмкіндігін қамтамасыз етеді.

Кірудің жаңа атауын құру. SQLServer кіруінің жаңа атауын құру үшін келесі әрекеттерді орындау керек:

1) *SQL Server Management Studio ортасын ашу* (Іске қосу/Барлық бағдарламалар/Microsoft SQL Server 2008 R2/SQL Server Management

Studio);

2) *ObjectExplorer* панелінде *<Сервер атауы>/Security* торабын ерекшелеп, мәнмәтіндік мәзірдің көмегімен *New/ Login* командасын таңдау керек (5.25-сурет);

3) Ашылған терезедегі *General* қосымша бетінен аутентификация әдісін таңдау керек: Windows аутентификациясы *(Windowsauthentication)* немесе SQLServer аутентификациясы (AQL*Serverauthenti- cation*)(5.26-сурет).

Windows аутентификация әдісі таңдалған болса, онда то требуется ввести новое имя входа в поле *Loginname* жолына кірудің жаңа атауын енгізу қажет немесе либо *Search* батырмасының көмегімен Windowsc пайдаланушы атауын таңдау керек.

5.25-сурет. SQL Server Management Studio көмегімен кірудің жаңа атауын құру

5.26-сурет. Аутентификация әдісін таңдау

Егер, SQLServer, аутентификация тармағы таңдалған болса, онда кіру атауынан басқа кіруге арналған құпиясөзді де енгізу қажет. SQLServer аутентификациясы ккезінде келесі опциялар да қолжетімді: *Құпия сөз саясатын пайдалануды талап ету, Құпиясөздің жарамдылық мерзімін көрсету және Пайдаланушы келесі кіру кезінде құпиясөзді өзгертуі керек.*

TransactSQL көмегімен кірудің жаңа атауын құру. Transact SQL көмегімен кірудің жаңа атауын құру үшін келесі әрекеттерді орындау керек:

1) *NewQuery* батырмасын басу арқылы немесе сұраныс мәтінінің аясындағы мәнмәтіндік мәзірдің аттас командасының көмегімен жаңа SQL-сұраныс құру керек (5.27-сурет);
2) сұраныс мәтінін енгізу жолына келесі мәтінді енгізу қажет:
   - Windows шынайылығын тексерумен кірудің жаңа атауын құру:

Create login < windows кіру атауы > from windows

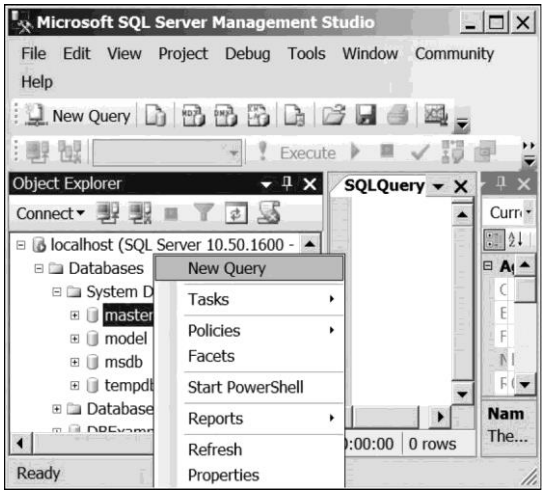
   - SQLServer шынайылығын тексерумен кірудің жаңа атауын құру (5.28-сурет):

Create login <кіру атауы>with password = '<құпиясөз>'

3) командалар панеліндегі Execute батырмасын басу арқылы немесе сұраныс мәтінінің аясындағы мәнмәтіндік мәзірдің аттас командасының көмегімен SQL-сұранысты орындау керек.

Мәліметтер базасы деңгейінің рөлін құру. SQLServer кірудің жаңа атауын құру үшін келесі әрекеттерді орындау керек: :

1) SQL Server Management Studio ортасын ашу керек (Іске қосу/Барлық бағдарламалар/Microsoft SQL Server 2008 R2/SQL Server Management Studio*)*



5.32. сурет. Бағана орнату үшін рұқсат

2) *ObjectExplorer* панелінде *<Сервер атауы>/<Мәліметтер базасының атауы>/Security* торабын ерекшелеп, мәнмәтіндік мәзірдің көмегімен *New/DatabaseRole* командасын таңдау керек (5.29-сурет);

3) ашылған терезеден жаңа рөлдің атауын, қолжетімділіктің еншіленетін құқықтарының нұсқаларын енгізу керек және құрылытан рөл үшін пайдаланушыларды таңдау керек (5.30-сурет);

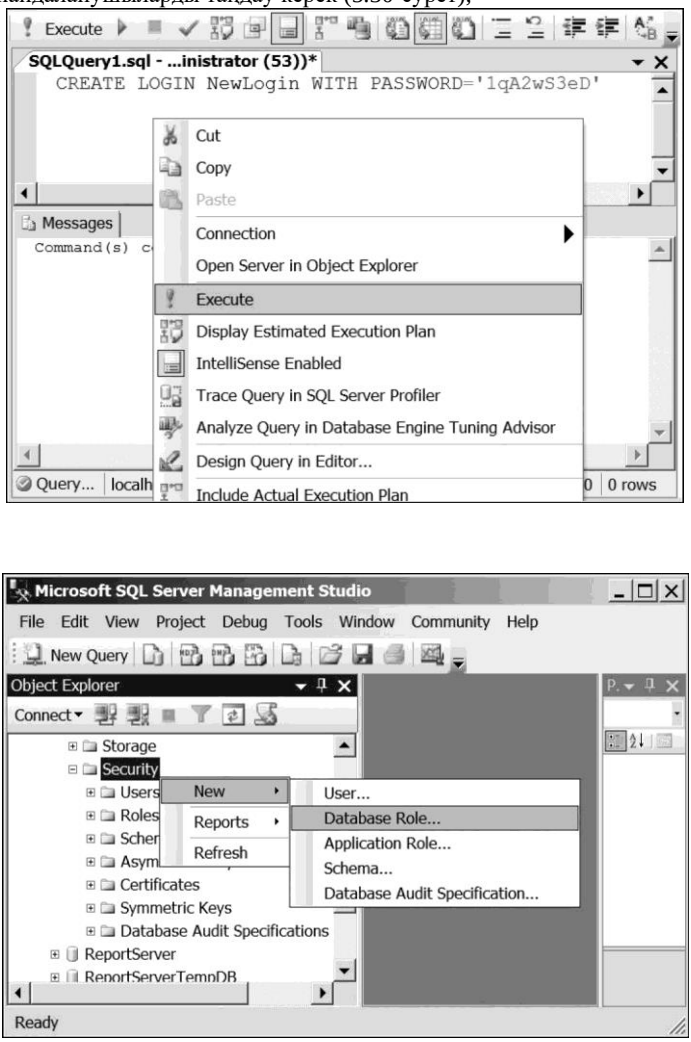
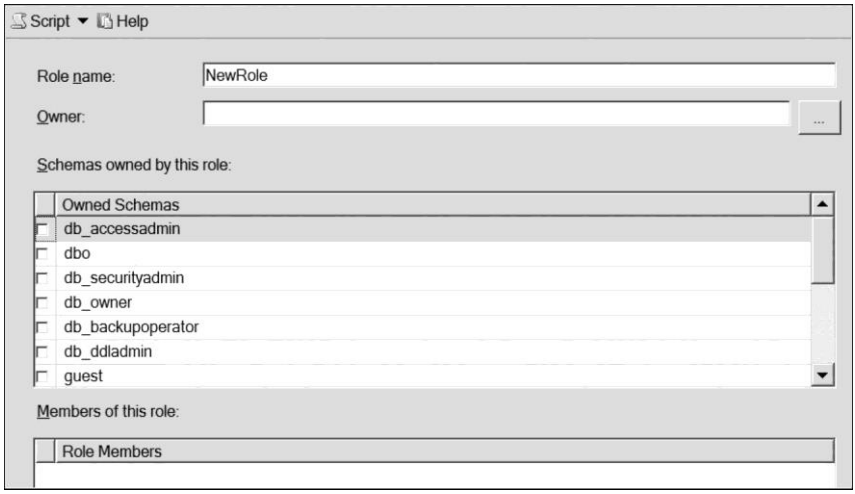


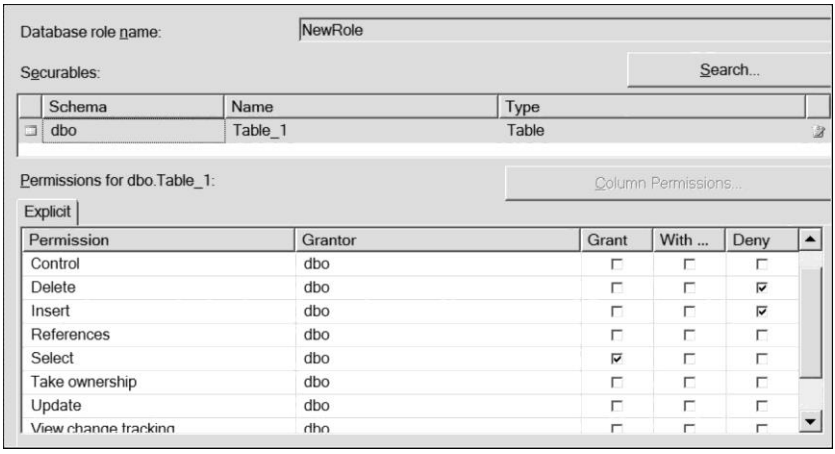
Рис. 5.29. Создание новой роли уровня базы данных

1) қорғалатын нысандардың қосымша бетінде *(Securables)*мәліметтер базасының түрлі нысандарына арналған қолжетімділіктің құқықтары мен

параметрлерін баптау. Жоғарғы жағы қолжетімділік нысандарын таңдауға арналған, ал астыңғысы – қолжетімділік параметрлерін баптауға арналған (5.31-сурет).



5.30-сурет. Мәліметтер базасы деңгейінің рөл құру терезесінің жалпы параметрлерінің қосымша беті



5.31-сурет. Мәліметтер базасының қорғалатын нысандарына қолжетімділікті баптаудың қосымша беті

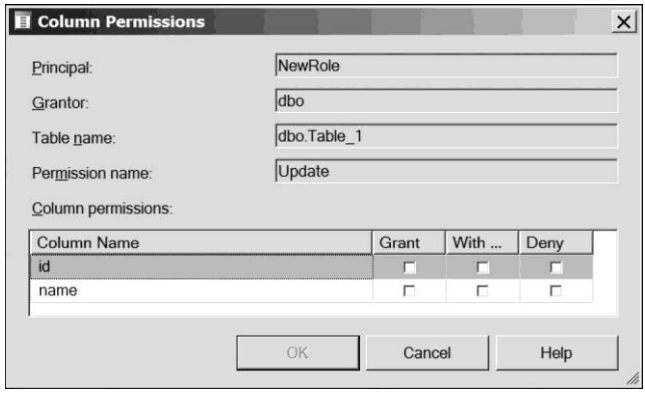
Мұнда кестенің жекелеген бағаналарына қолжетімділік құқытарын баптау мүмкіндігі ұсынылады (сәйкес шешімдерді таңдау кезінде іске қосылатын *ColumnPermissions*батырмасы). Бағаналарға арналған рұқсаттарды баптау

терезесі 5.32-суретте көрсетілген.

Мәліметтер базасы деңгейінің рөлін құрк SQL-сұраныстардың көмегімен орындауға болады (нақты мәліметтер базасы үшін):

■ *sp_addrole* сақталатын рәсімінің көмегімен:

exec sp addrole <рөл атауы>;



■ *CreateRole* командасының көмегімен:

CreateRole<рөл атауы>.

Рұқсаттар, сондай-ақ, Transact-SQL командасының көмегімен берілуі мүмкін. Мысалы, жаңа рөл құру және 5.32-суреттегіге ұқсас рұқсаттар тағайындау үшін келесі сұранысты орындау қажет:

```
Create Role NewRole
Grant Select on Tablel to NewRole
Deny Delete, Insert on Tablel to NewRole
```

Мәліметтер базасының жаңа пайдаланушысын құру. Мәліметтер базасының жаңа пайдаланушысын құру үшін клеесі әрекеттерді орындау керек:

1) *SQL Server Management Studio ортасын ашу керек* (Іске қосу/Барлық бағдарламалар/Microsoft SQL Server 2008 R2/SQL Server Management Studio);
2) *ObjectExplorer* панелінде *<Сервер атауы >/<Мәліметтер базасының атауы>/Security* торабын ерекшелеп, мәнмәтіндік мәзірдің көмегімен *New*/*User* командасын таңдау керек;
3) ашылған терезеде жаңа пайдаланушының атауын енгізіп, логин атауын (міндетті жол), қолжетімділіктің еншіленетін құқықтарының нұсқаларын таңдау керек және құрылып жатқан мәліметтер базасы пайдаланушысының рөлін таңдау керек (5.33-сурет). Қорғалатын нысандардың қосымша беті

(Securables) мәліметтер базасы деңгейінің рөл құру терезесінің аттас қосымша бетіне ұқсас.

SQL-сұраныстар құралдарының көмегімен мәліметтер базасының жаңа пайдаланушысын құру үшін мына командалардың біреуін орындау керек:

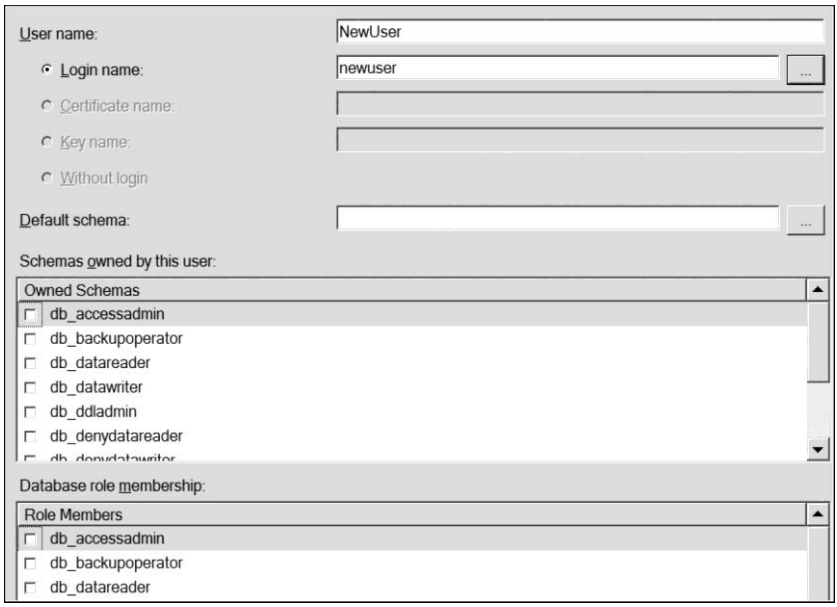
- *sp_adduser* сақталатын рәсімінің көмегімен:

exec sp adduser <пайдаланушыларға атау

- *CreateUser* командаының көмегімен:

CreateUser<пайдаланушыларға атау

Пайдаланушы үшін рөлді тағайындау үшін пайдаланушының мәнмәтіндік мәзірінің *Қасиеттер (Properties)* командасы арқылы қолжетімді болатын пайдаланушы қасиеттері терезесін пайдалану керек (5.34-сурет). Пайдаланушы қасиеттерінің терезесі мәліметтер базасының жаңа пайдаланушысын құру терезесіне ұқсас. Пайдаланушыға рөл тағайындау үшін *Жалпы (General)* қосымша бетінен тізімдегі сәйкес рөлді таңдау керек.



5.33-сурет. Мәліметтер базасының жаңа пайдаланушысын құру терезесі

Мәліметтер базасын пайдаланушыға рөл тағайындау *sp_addrolemember* сақталатын рәсімінің көмегімен SQL-сұраныс құралдарымен жүзеге асырылуы мүмкін:

execspaddrolemember<рөл атауы>, <пайдаланушылар атауы

БАҚЫЛАУ СҰРАҚТАРЫ

1. Internet Information Services деген не?
2. IIS қызметтер конфигурацияларын қалай басқаруға болады?
3. Конфигурацияның ұсынылуы деген не және ол не үшін қолданылады?
4. Конфигурациялық файлдарды редакциялаудың қандай әдістерін білесіз?
5. IIS 7-тегі Windows Management Instrumentation қандай міндеттерді шешеді?
6. Оқиғаларды журналдаудың баптаулары қалай орындалады?
7. Сервер конфигурациясының өзгеруі оқиғаларын бақылау кезінде қандай ақпараттарды сақтау талап етіледі?
8. MicrosoftIIS7 платформасы IP-мекенжайлар бойынша серверге қолжетімділікті шектеудің қандай құралдарын ұсынады?
9. Мәліметтер жолдауды қандай технологиялар оңтайландыруға мүмкіндік береді?
10. MicrosoftIIS қызметтерінің құралдарымен мәліметтерді кэштеуді баптау процесінің мәні неде?
11. Үдемелі және статикалық Web-парақшаларды кэштеудің айырмашылықтары неде?
12. Файлдық сервердің негізгі қызметтері қандай?
13. WindowsServer 2008-тегі файлдық сервердің рөлін орнату қалай орындалады?
14. Файлдық сервер аудиті қандай міндеттерді шешуге мүмкіндік береді?
15. Файлдық сервер аудитінің саясатын баптау мәнісі неде?
16. Ортақ ресурске арналған рұқсаттар қандай деңгейлерде анықталады?
17. Файлдық сервердің ресурстар диспетчері қандай міндеттерді шешу үшін қолданылады?
18. Пошталық сервердің қандай негізгі қызметтерін білесіз?
19. Пошталық сервердің көмегімен жолданатын ақпараттың мониторингі қалай жүргізіледі?
20. MicrosoftExchangeServer2010-дағы модельдеу механизмі жұмысының қағидалары қандай?
21. MicrosoftExchangeServer2010-дағы пошталық аккаунттарға қолжетімділік құқытарын басқару қандай әдістермен орындалады?
22. Пошталық жәшікке толық қолжетімділікке рұқсаттарды орнату қалай орындалады?
23. SQLServer2008-де конфигурацияны бақылау қандай дәрежелерде қамтамасыз етіледі?
24. SQLServer2008 конфигурациясын бақылаудың қадағаланатын оқиғаларын қандай топтарға жіктеуге болады?
25. Аудит нәтижелерін бекіту қандай әдістермен орындалуы мүмкін?
26. Аудиттің жаңа сипаттізімін құру қалай жүргізіледі?
27. Мәліметтер базасын резервтік көшірмелеу және қалпына келтірудің механизмімен қандай негізгі мақсаттар қамтамсыз етіледі?
28. Мәліметтер базасында сақталатын ақпарат бүтіндігінің бұзылуының

негізгі себептері неде?

29. SQLServer2008-де мәліметтерге қолжетімділікті басқару кезінде қарастырылатын қатысушылардың негізгі дәрежелері қандай?
30. Түрлі субъектілер үшін қолжетімділік құқықтарын басқару қандай әдістермен орындалуы мүмкін?

Әдебиеттер тізімі

Ресей Мемтехкомиссиясы. Жетекші құжат. Ақпаратқа рұқсат етілмеген қолжетімділіктен қорғаныш. Терминдер мен анықтамалар. — М. : ГТК, 1992.

Ресей Мемтехкомиссиясы. Жетекші құжат. Автоматтандырылған жүйелер. Ақпаратқа рұқсат етілмеген қолжетімділіктен қорғаныш. Автоматтандырылған жүйелердің жіктелуі және ақпаратты қорғау жөніндегі талаптар. — М. : ГТК, 1992.

Ресей Мемтехкомиссиясы. Жетекші құжат. Есептеуіш техниканың құралдары. Ақпаратқа рұқсат етілмеген қолжетімділіктен қорғаныш. Ақпаратқа РЕҚ-тен қорғану көрсеткіштері. — М. : ГТК, 1992.

Ресей Мемтехкомиссиясы. Жетекші құжат. Есептеуіш техниканың құралдары. Желіаралық экрандар. Рұқсат етілмеген қолжетімділіктен қорғану көрсеткіштері. — М. : ГТК, 1997.

Белов Е. В. Ақпараттық қауіпсіздік негіздері: оқу құралы / Е. В. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — М. : Жедел желі — Телеком, 2006. — 544 б.

Галатенко В. А. Ақпараттық қауіпсіздік стандарттары: дәрістер курсы: оқу құралы. — 2-ші бас. / В. А. Галатенко ; В. Б. Бетелина ред-н— М. : Ақпараттық технологиялардың интернет-университеті, 2006. — 264 б.

Голиков А. М. Ақпараттық қауіпсіздік негіздері: оқу құралы / А.М.Голиков. — Томск : ТУСУР, 2007. — 154 б.

Граннеман Б. Linux. Қажетті код және командалар. Қалта анықтамалығы / Б.Граннеман. — М. : Вильямс, 2010. — 416 б.

Запечников Б. В. Ақпараттық жүйелердің ақпараттық қауіпсіздігі: оқулық. — 2 т. Т. 1. Қауіптер, әлсіздіктер, шабуылдар және қорғанышқа арналған тәсілдер / Б.В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. — М. : Жедел желі — Телеком, 2006. — 536 б.

Колисниченко Д. Н. Linux желілік әкімшісінің өздігінен үйретушісі/ Д.Н. Колисниченко. — СПб. : БХВ-Петербург, 2011. — 544 б.

*Кришнамурти Б.*Web-хаттамалар. Теория мен тәжірибе / Б. Кришнамурти, Дж. Рексфорд. — М. : БИНОМ, 2002. — 592 с.

Лимончелли Т. Жүйелік және желілік әкімшіліктендіру. Тәжірибелік нұсқаулық / Т. Лимончелли, К. Хоган, Б.Чейлап. — М. : Символ-Плюс, 2009. — 546 б.

Манн Б. Linux. TCP/IP/ желілерін әкімшіліктендіру. Б. Манн, М. Крелл. — М. : Бином-Пресс, 2012. — 672 б.

Нортроп Т. WindowsServer2008 желілік инфрақұрылымын жобалау. Microsoft оқу курсы/ Т. Нортроп, Дж.Макин. — М. : Орыс редакциясы, 2009. — 592 б.

Олифер В. Г. Компьютерлік желілер. Қағидалар, технологиялар, хаттамалар..

— 4-ші баб. / В. Г. Олифер, Н. П. Олифер. — СПб. : Питер, 2010. — 944 б.

*ОринТ.*Windows Server 2008: Enterprise Administration / Т. Орин, Д. Поличелли, И. Маклин, Дж. Макин және т.б. — М. : Орыс редакциясы, 2011. — 528 б.

Смирнова Е. В. Коммутацияланатын компьютерлік желілерді құру: оқу құралы / Е. В. Смирнова, А. В. Пролетарский, И. В. Баскаков, Р. А. Федотов. — М. : БИНОМ. Білім зертханасы, 2011. — 367 б.

Старовойтов А. А. LINUX-тегі желі. Жобалау, салу, пайдалану / А. А. Старовойтов. — СПб. : БХВ-Петербург, 2006. — 288 б.

Суровов А.М. Желіаралық экрандар: оқу құралы / А.М.Суровов, А. В. Пролетарский, И.В. Баскаков. — М. : Рудомино кітап орталығы, 2011. — 288 б.

Фленов М. Хакер көзімен қарағандағы Linux (+ CD-ROM) / М.Фленов. — СПб. : БХВ-Петербург, 2010. — 480 б.

Шаньгин В. Ф. Компьютерлік жүйелер мен желілердегі ақпаратты қорғау / В. Ф. Шаньгин. — М. : ДМК Пресс, 2012. — 592 б.

Шаньгин В. Ф. Компьютер ақпараттарын қорғау. Тиімді әдістер мен құралдар / В. Ф. Шаньгин. — М. : ДМК Пресс, 2008. — 544 б.

Шаньгин В. Ф. Компьютерлік жүйелер мен желілердегі ақпараттық қорғаныс: оқу құралы/ В.Ф.Шаньгин. — М. : Форум ; Инфра-М, 2008. — 416 б.

Щербаков А. Ю. Заманауи компьютерлік қауіпсіздік. Теориялық негіздер. Практикалық аспектілер: оқу құралы / А. Ю. Щербаков. — М. : Кітап әлемі, 2009. — 352 б.

Мазмұны

Алғысөз 4
Кіріспе 9

I БӨЛІМ

КОМПЬЮТЕРЛІК ЖЕЛІЛЕРДІҢ БАҒДАРЛАМАЛЫҚ ҚАМСЫЗДАНДЫРУЫН ПАЙДАЛАНУ

1-тарау. Web-серверді орнату 22

1.1. Web-индустрияның дамуы 22
1.2. Web-сервер ұғымы 24
1.3. Жеңіл Web-серверлер 26
1.4. Web-серверді орнату 31
1.5. Аппараттық базаны таңдау 33
1.6. Web-серверді конфигурациялау 36
1.7. Серверді қосу, қайта қосу және тоқтату 51
1.8. Бірнеше Web-тораптардың хостингі 55
1.9. Тіркеу және мониторинг 64
Қауіпсіздік 74
Үдемелелі Web-парақшалар 89
Мәліметтер базасымен өзара әрекеттестік 103

2-тарау. Брандмауэрді орнату және параметрлері 108

2.1. Брандмауэрдің негізгі қызметтері 108
2.2. Брандмауэрлер түрлері 109
2.3. Фаерволмен шешілмейтін проблемалар 110
2.4. Firewall-ды жүзеге асыру 111
2.5. Linux TCP/IP Firewall 119
2.6. Linux IP Firewall орнату және іске қосу 123
2.7. Кестелер мен тізбелерді өту тәртібі 125
2.8. IP Firewall Chains (2.2 ядро) 135
2.9. Netfilter және IP кестелер (2.4 ядро) 145
2.10. IP Accounting 153
2.11. IP Accounting баптауы 154
2.12. IP Masquerade және Network Address Translation 164

II БӨЛІМ
КОМПЬЮТЕРЛІК ЖҮЙЕЛЕРГЕ ҚЫЗМЕТ КӨРСЕТУ ЖӘНЕ ӘКІМШІЛІКТЕНДІРУ

3-тарау. Ақпаратты қауіпсіз жолдау үшін сервер мен жұмыс станцияларын баптау 174
3.1. DCHP Server қызметінің баптауы.....174
3.2. DNS қызметінің баптауы.....191
3.3. Доменнің ақпараттық жүйесінің баптауы 205
3.4. Доменнің топтық саясатының баптауы 222
3.5. Ақпаратты қауіпсіз жолдауды конфигурациялау 233

4-тарау. Жергілікті және жаһандық желілерге қолжетімділікті ұйымдастыру 243
4.1. Бағыттаудың негізгі қағидалары 243
4.2. Сымсыз қосылу бойынша желілерге қолжетімділікті ұйымдастыру.....252
4.3. Кэштеуші прокси-серверді құру 253
4.4. Жаһандық желілерге қолжетімділік кезінде қорғанысты қамтамасыз ету.....260

5-тарау. Web-серверді, файлдық серверді, пошталық серверді, SQL-серверді пайдалануды бақылау және сүйемелдеу.....271
5.1. Web-серверді бақылау және сүйемелдеу 271
5.2. Файлдық серверді бақылау және сүйемелдеу 279
5.3. Пошталық серверді бақылау және сүйемелдеу.....286
5.4. SQL- серверді бақылау және сүйемелдеу.....294

Әдебиеттер тізімі 313

Оқу басылымы

Баранчиков Алексей Иванович,
Баранчиков Павел Алексеевич,
Громов Алексей Юрьевич

Желілік әкімшілендіруді ұйымдастыру

Оқулық

Редакторы Л. *В. Толочкова*
Компьютерлік беттеу: *Р. Ю. Волкова*
Корректор Л. В. *Гаврилина*

Бас. № 101116970. Басуға қол қойылды 01.07.2015. Пішімі 60 х 90/16.
Гарнитура «Балтика». Офесттік қағаз. Офсеттік баспа. Шар. Бас. П. 20,0.
Тиражы 1000 дана. Тапсырыс №

«Академия» баспа орталығы» ЖШҚ. www.academia-moscow.ru129085, Мәскеу,
Бейбітшілік даң-ы, 101В, құр.1.
Тел./факс: (495) 648-0507, 616-00-29.
Санитарлық-эпидемиологиялық қорытынды 25.05.2015 ж. № РОСС RU. АЕ51. Н 16679

Баспа ұсынған электронды тасымалдағыштардан «Саратов полиграфкомбинаты» ААҚ-да
басып шығарылды, www.sarpk.ru410004, Саратов қ., Чернышевский көш., 59.