nodrošinājuma izmantošanā no jebkura zemeslodes punkta, kur ir Interneta pieslēgums. Tāpat piedāvājamā arhitektūra paredz iespēju radīt vairākus Vadības centrus, respektīvi, virtuālās augstskolas, kas izmanto kopīgu metodisko nodrošinājumu. Tas viss paver plašas iespējas starptautiskai sadarbībai.

Literatūra

1. Kiscenko A., Onzevs O., Zommers J. Methodological Support for Economical Education by Using Information Technologies. // Proc, of Scientific Conference "Rural Areas Development in the North–western Macroregion of Poland under Conditions of State Reforms and European Integration", Szczecin, Poland, 21–24 June 1999, Volume II, pp. 219–223.
2. Kiscenko A., Onzevs O., Petersons L. Business Administration Studies via Internet // Book of Abstracts of 6th International Conference on Technology Supported Learning & Training "ONLINE EDUCA BERLIN", Hotel InterContinental, Berlin, November 30 – December 1, 2000, pp. 52–54.
3. Onževs O., Vārslava I., Kiščenko A. Informācijas apmaiņas nodrošināšana datorizētā tālmācības studiju proces // Starptautiskā zinātniskā konference BALTIJAS VALSTU INTEGRĀCIJAS PROBLĒMAS CEĻĀ UZ EIROPAS SAVIENĪBU, Rēzekne, 2000. gada 2.–3. marts, 174.–178. lpp.

DATORTĪKLA ADMINISTRĒŠANAS UN KONTROLES SISTĒMAS IZVEIDE UZ OPERĒTĀJSISTĒMAS "LINUX" BĀZES
DEVELOPMENT OF LINUX–BASED NETWORK ADMINISTRATION AND CONTROL SYSTEM

Vitauts Stočka, Daugavpils Pedagoģiskā universitāte

Abstract. *Administration and control of medium–sized and large computer networks is one of the most important tasks for any organization. Existing solutions are either too expensive for educational institutions or consists of many separate programs with little or no centralized managements.*

This work describes system in development based on "Linux" operational system and popular open standards. The central part of the system is LDAP database for information about servers, computers, users etc. This database is used by many less or more independent modules, including mail, proxy and other Internet servers. Access to these services is controlled by firewalls and specialized client/server authorization system, which is needed to prevent password sniffing and other methods of unauthorized access.

System is managed from a centralized web–based administration interface.

System is under development and will be implemented in several stages, module by module.

Problēmas izklāsts

Jebkurā pietiekoši lielā datortīklā agri vai vēlu rodas virkne uzdevumu un problēmu, kuru veiksmīga risināšana ir atkarīga no tīkla centralizētas administrēšanas un kontroles iespējām. Pieaugot tīklam pieslēgto datoru skaitam, pieaug ne vien kopējais informācijas plūsmas apjoms, bet arī centrālo serveru un ārējo līniju (Interneta pieslēguma) noslogojums. Ja organizācijas vadība ir ieinteresēta saglabāt kontroli pār kopējo tīkla attīstību, tīkla uzturēšanas izmaksām un tīkla lietotāju darbību, ir jādomā par vienotas, centralizētas tīkla uzraudzības sistēmas izveidi. Šādā gadījumā atsevišķi tīkla segmenti var tikt veidoti un uzraudzīti atsevišķi,

ISBN 9984 - 585 - 36 - 0

taču kopējo tīkla struktūru, tā elementus un to mijiedarbību nosaka daži mezgla punkti, kas tiek vadīti centralizēti, izmantojot vienotu informācijas datu bāzi.

Šajā darbā tiek izklāstīti apsvērumi un iestrādnes, kas saistītas ar centralizētas tīkla vadības sistēmas izveidi Daugavpils Pedagoģiskajā universitātē. Sistēma pašlaik tiek izstrādāta, taču atsevišķi tās elementi jau darbojas vai tiek testēti.

Iespējamie risinājumi

Centralizētas tīkla vadības sistēmas izveide nav jauns uzdevums, un dažādu līmeņu un sarežģītības pakāpes sistēmas tiek veiksmīgi izmantotas. Tomēr vairums šādu sistēmu vai nu ir ļoti dārgas, vai arī risina tikai daļu no uzdevumiem, tāpēc nav pieņemamas kā risinājums mācību iestādēm.

Tajā pat laikā eksistē ļoti daudz bezmaksas programmu, kas risina atsevišķus ar tīkla administrēšanu un kontroli saistītus uzdevumus. Dažas no šīm programmām pēc savām iespējām neatpaliek no analogiem komerciāliem risinājumiem, taču tās prasti nav salāgotas savā starpā, trūkst lietotāja dokumentācijas, un tas negatīvi ietekmē šo programmu izplatību. Šādas bezmaksas jeb atvērtā sākumkoda programmas ir pieejamas jebkuru ar tīkla vadību saistītu uzdevumu risināšanai.

Vairums šo programmu ir pieejamas bezmaksas operētājsistēmai "Linux" vai citām "Unix" saimes sistēmām. Ņemot vērā autora ilgstošo pieredzi darbā ar "Linux", kas tiek izmantots jau kopš 1994. gada, kā arī iestrādnes uz "Linux" bāzes, kā optimālākā platforma vienotas tīkla vadības sistēmas izveidei tika izvēlēta tieši "Linux" operētājsistēma. Paredzams, ka atsevišķas sistēmas daļas var tikt realizētas uz citu operētājsistēmu bāzes. Kā piemērus var minēt uz "DOS" bāzes veidotus maršrutizatorus "IP–Route" un "FreeBSD" risinājumus, kas dažās situācijās uzrāda labāku ātrdarbību. Kopumā sistēma būs veidota uz "Linux" bāzes, taču samērā viegli pārnesama uz jebkuru citu "Unix" saimes sistēmu. Administratora interfeisu ir paredzēts veidot uz WWW bāzes, kas ļauj sistēmai piekļūt no jebkuras vietas neatkarīgi no izmantotās operētājsistēmas un datora atrašanās vietas.

Sākotnējā situācija Daugavpils Pedagoģiskajā universitātē

DPU datortīkla infrastruktūras pamatā ir vairāki "Linux", "AIX" un "IRIX" serveri, kā arī citi tīkla aktīvie elementi, tajā skaitā "Cisco", "Linux", "IP–Route" maršrutizatori, "3COM" un citu ražotāju komutatori un koncentratori. Galvenos tīkla servisus nodrošina "Linux" serveris, kurā ir reģistrēti lietotāju konti, tiek glabāts lietotāju pasts un mājas lapas. Šis serveris kalpo arī kā autorizācijas serveris vairākiem proxy serveriem, kas kontrolē lietotāju piekļūšanu Internet tīklam un veic trafika uzskaiti. Saskaņā ar DPU pieņemtajiem tīkla lietošanas noteikumiem, visiem DPU darbiniekiem un studentiem ir jānoslēdz līgums, lai iegūtu lietotāja vārdu un paroli, kas vienlaicīgi nodrošina gan e–pasta adresi, gan iespēju lietot Internetu. Darbs Internetā tiek uzskaitīts, un par ienākušo starptautisko trafiku lietotājiem ir jāmaksā.

Kaut gan šāda kārtība nedaudz ierobežo studentu iespējas izmantot tīklu, tomēr esošā pieredze liecina, ka ievērojamu saņemtās informācijas daļu sastāda ar studijām un darbu nesaistīta informācija, tāpēc izmantojamo uzskaites un apmaksas modeli var uzskatīt par samērā efektīvu līdzekli neracionāla tīkla noslogojuma ierobežošanai. DPU datortīkla izmantošanas noteikumi nenosaka saņemamās informācijas filtrēšanu, tāpēc netiek bloķēta piekļūšana nevienai tīkla lapai. Tomēr sistēmas struktūra paredz šādu iespēju, kas var tikt izmantota skolās.

Ar tīkla lietošanas noteikumiem saistītie jautājumi neietilpst šī darbā tematikā, un piedāvātā tīkla vadības sistēma būs elastīgi pielāgojama dažādiem nosacījumiem, tajā skaitā arī

ISBN 9984 - 585 - 36 - 0

noteiktu tīkla resursu bloķēšanai, atsevišķu lietotāju darbības ierobežošanai un citiem specifiskiem gadījumiem.

Veidojamās sistēmas vispārējā struktūra

Sistēma tiek veidota pēc moduļu principa, izmantojot vienotu informācijas datu bāzi un administrēšanas interfeisu.

Datu bāze glabā visu nepieciešamo informāciju par datortīkla elementiem: serveriem, darba stacijām, maršrutizatoriem, komutatoriem u.c, kā arī par lietotājiem. Datubāzes veidošanai tiek izmantots vispārpieņemts standarts LDAP (Lightweight Directory Access Protocol), kas tiek izmantots arī "Microsoft Active Directory" risinājumā operētājsistēmā "Windows 2000". Kaut gan DPU tīkla infrastruktūrā galvenokārt tiek izmantoti "Unix" saimes serveri, tomēr savietojamībai ar "Windows" tiek pievērsta liela uzmanība. "Linux" vidē populārākais ir serveris "OpenLDAP", kas arī tiek izmantots sistēmas vajadzībām. Daudzas "Linux" programmas ļauj izmantot LDAP datu bāzi tīkla informācijas glabāšanai, tomēr "LDAP" nav guvis pārāk plašu izplatību, jo ir salīdzinoši sarežģīts un tā izmantošana maziem tīkliem prasa pārāk lielu darba ieguldījumu.

Sistēmas moduļi paredzēti konkrētu uzdevumu risināšanai. Vairums moduļu ir "parastas" programmas, kas konfigurētas vienotas "LDAP" datubāzes izmantošanai, tomēr tiek strādāts arī pie dažu specifisku modeļu programmēšanas.

Galvenie moduļi ir pasta sistēma un proxy serveri. Atšķirībā no agrāk izmantotās pasta sistēmas, kas paredzēja katram lietotājam veidot "reālu" "Linux" lietotāja kontu, jaunā sistēma balstās uz "virtuālām" pastkastēm. Rezultātā lietotājiem netiek veidoti reāli operētājsistēmas konti. Adreses eksistence tiek pārbaudīta "LDAP" datubāze, no kuras tiek noskaidrots arī katalogs, kurā jāsaglabā saņemtais pasts. Šāds risinājums ļauj ne vien ērtāk un elastīgāk administrēt lietotājus, bet arī palielina sistēmas drošību, jo reālu lietotāju kontu izveide vienmēr ir saistīta ar kompromisiem drošības jomā. Pasta saņemšanai varēs izmantot "POP3" un "IMAP4" protokolus, kā arī "WWW" interfeisu.

Nākamais ir proxy serveru modulis, kas veic Interneta lietotāju autorizāciju un trafika uzskaiti. Šis modulis ir gandrīz pilnībā izstrādāts, un tā agrākas versijas tiek ilgstoši izmantotas un uzlabotas. Moduļa pamatā ir proxy serveris "Squid". Šis serveris izmanto "LDAP", kā arī ļauj pieslēgt papildus programmas saņemamās informācijas satura kontrolei. Pašlaik DPU tiek izmantoti vairāki proxy serveri, kas veido vienotu sistēmu, taču katrs ir paredzēts specifiskām vajadzībām un nedaudz atšķiras pēc piedāvātajām iespējām. Visas saņemtās informācijas žurnāls jeb "log" fails, ieskaitot lietotāja vārdu, datoru pie kura strādājis lietotājs, saņemtā faila URL un izmēru, tiek glabāts failā un vēlāk izmantots statistikas aprēķināšanai. Aprēķinot statistiku, tiek ņemta vērā servera atrašanās vieta – Latvijā vai ārzemēs.

Paredzēts, ka operatīvas statistikas veidošanai "Squid" žurnāls automātiski tiks saglabāts "MySQL" datu bāzē. Tas ļaus katram lietotājam jebkurā brīdī saņemt statistiku par savu darbu tīklā, bet tīkla administratoriem būs iespēja kontrolēt kopējo situāciju un konstatēt dažādus tīkla izmantošanas pārkāpumus. Pašlaik ir izstrādāta programma, kas katru nakti lietotājiem pa e–pastu izsūta informāciju par iepriekšējās dienas aktivitātēm. Šī pati informācija ir pieejama arī "WWW" lapā, taču šis modulis pašlaik ir atslēgts, lai atrisinātu dažus ar drošību saistītus jautājumus.

"LDAP" datu bāzē paredzēts glabāt arī informāciju par visiem tīkla datoriem. Šo informāciju varēs izmantot pārējo tīkla servisu vadībai un kontrolei, piemēram, ierobežojot atsevišķu lietotāju darbu no noteiktiem datoriem, bloķējot atsevišķus datorus noteiktos laika posmos, un tml. Šim nolūkam tiks izmantotas "Squid" papildprogrammas, kā arī ugunsmūri,

ISBN 9984 - 585 - 36 - 0

kas bloķēs datu plūsmu starp serveriem un noteiktiem tīkla datoriem. Pašlaik "Linux" pieejamie ugunsmūru risinājumi neparedz "LDAP" datu bāzes izmantošanu, tāpēc ir uzsākts darbs pie programmas dinamiskai ugunsmūra konfigurācijai mainīšanai pēc "LDAP" vai citu konfigurācijas datu izmaiņām.

Pašlaik tiek izstrādāti programmu prototipi un veikti eksperimenti, lai izstrādātu jaunu lietotāju autorizācijas mehānismu, kura pamatā būs vairāklīmeņu pieejas kontrole. Agrāk izmantotās metodes lietotājiem ļauj no jebkura datora inicializēt savienojumu ar jebkuru nepieciešamo tīkla servisu, piemēram, pasta vai proxy serveri, un tad šis serviss ar saviem līdzekļiem veic lietotāja autorizāciju. Diemžēl pieredze rāda, ka šāda metode nav droša, kā rezultātā lietotāju paroles nonāk negodīgu cilvēku rokās. Lai to novērstu, ir paredzēts ieviest papildus autorizācijas līmeni. Speciāla ugunsmūra programma bloķēs jebkura datora pieeju citiem tīkla resursiem, izņemot speciālu autorizācijas servera portu. Lai piekļūtu tīklam, lietotājam vispirms būs jāpieslēdzas šim autorizācijas serverim, no kura tiks saņemta speciāla autorizācijas programma. Programma izmantos "LDAP" datu bāzē glabāto informāciju par datoriem, lietotājiem un viņu tiesībām. Lietotājs autorizācijas programmā varēs ievadīt speciālu autorizācijas kodu un norādīt konkrētu servisu vai servisus, ko viņš vēlas izmantot šī darba seansa laikā. Ja ievadītā un pieprasītā informācija atbildīs datubāzē glabātajām tiesībām, ugunsmūris atvērs pieeju pieprasītajiem servisiem. Tiklīdz lietotājs aizvērs autorizācijas programmu vai arī noteiktu laiku nebūs izmantojis tīklu, ugunsmūris aizvērs kanālu, un autorizācija būs jāatkārto. Šis ugunsmūra un autorizācijas modulis ir būtiskākais elements tīkla drošības nodrošināšanai, jo tas kalpos kā filtrs starp lietotāju un visiem pārējiem tīkla servisiem. Tādējādi kopējā sistēmā iespējams integrēt arī tādas programmas, kas tieši nemijiedarbojas ar "LDAP" datu bāzi. Autorizācijas programma sastāvēs no divām daļām. Lietotājam tiks izsūtīta "Java" programma, kas ļaus ievadīt autorizācijas kodu, paroli un izvēlēties vajadzīgos servisus. Lai nebūtu iespējams pārtvert ievadāmās taustiņu kombinācijas, daļu no autorizācijas kodiem lietotājam būs jāievada grafiski, ar peles palīdzību. "Java" programma nepārtraukti apmainīsies ar informāciju ar autorizācijas serveri. Autorizācijas serveris tiek programmēts "Python" valodā, izmantojot asinhrono komunikāciju bibliotēku. "Python" tika izvēlēta kā augsta līmeņa, kas ievērojami atvieglo sarežģītu uzdevumu programmēšanu, tajā pašā laikā saglabājot labu ātrdarbību, iespēju izmantot datu bāzes un visus tīkla protokolus. Informācijas apmaiņai ar klientam izsūtāmo autorizācijas programmu tiek izstrādāts speciāls datu apmaiņas protokols. Paredzams, ka šis protokols tiks nepārtraukti uzlabots un papildināts. Pašlaik izstrādāta vienkārša protokola versija, kas ļauj veikt autorizāciju un aizvērt ugunsmūra portus, ja autorizācijas programma klienta datorā tiek aizvērta.

Kopsavilkums

Šeit aprakstīti tikai daži no tīkla vadības sistēmas moduļiem, kas kopumā var nodrošināt efektīvu tīkla darbu un lietotāju uzraudzību jebkurā vidējā vai lielā datortīklā. Pašlaik turpinās struktūras izstrāde, atsevišķu moduļu vai to prototipu veidošana un ar to saistītie eksperimenti. Sistēma nav monolīta, tāpēc atsevišķus moduļus paredzēts ieviest pakāpeniski, un to pilnveidošana netiks pārtraukta arī pēc ieviešanas.

Paredzams, ka sistēmas ieviešanas gaitā radīsies jauni atzinumi, kuri tiks izklāstīti turpmākajos darbos.

Literatūra

1. Зиглер, Роберт Л. Брандмауэры в Linux. – М.: Издательский дом «Вильямс», 2000.
2. Building Scalable ISPs with open-source softwares, http://www.linuxfocus.org/English/September/2000/article173.shtml

ISBN 9984 - 585 - 36 - 0