УДК 004.7

Шаршембаев Б., Майтыков Т.
Кыргыз - Түрк Манас университети

SQUID ПРОКСИ СЕРВЕР НЕГИЗИНДЕ ВЕБ ТРАФИКТИН ОНЛАЙН МОНИТОРИНГИ ЖАНА ЭСЕБИН АЛУУ

Акыркы жылдары Интернеттин экспоненциалдык өсүп өнүгүүсү байкалууда жана информациондук революциянын башаты болуп келе жатат. Күндөн күнгө көптөгөн Интернет сервистер пайда болууда. Бул сервистер ар түрдүү кызмат, маалымат, тейлөөлөрдү камтышат. Ар бир сервис ар түрдөгү, ар көлөмдөгү трафикти жаратат жана бул трафиктин изилдөөсүнүн негизинде дагы сапаттуу, дагы илгери тейлөөлөрдү жаратуусу мүмкүн. Макалада изилдөөдө ушул проблемаларды чечүүдө жаралган кыйынчылыктарды, инструменттерди, методдорду дагы терең кароо максаттары каралган. Конкреттүү SQUID прокси сервер базасында веб трафиктин онлайн мониторинги жана эсеби жүргүзүлгөн.

Кириш сөз

Бүгүнкү күндө веб трафиктин көптөгөн анализаторлору бар. Кээбир трафик анализаторлор өз алдынча система түрүндө иштешет, мисал катары UserGate[1], LabrisWebfilter[2] программалары (ичинде прокси сервер функциясы бар). Мындан сырткары веб трафикти анализдөө үчүн прокси сервердин лог файлдарын анализдөө принцибине негизделген популярдуу программалар бар, мисал катары SQUID[3] + SARG[4] программалары.

Өз алдынча иштеген трафик анализаторлор (UserGate, LabrisWebfilter) кошумча тейлөө талап кылышат, ички код жабык болот, жана жаңы түрдөгү отчет жаратуу үчүн фирмага кайрылуу зарыл. Бирок коду ачык прокси серверлер бар, жана алардын жараткан протоколдук файлдары да ачык, жана бул файлдын негизинде оңой эле отчет түзүүгё мүмкүн. Мисал катары SQUID прокси серверде бир нече лог-анализаторлор жазылган. Көбүнчөлөрү сервер администраторлор тарабынан жазылып, колдон колго өтүп жайылып таралган.

Проблема

Бүгүнкү күндө бар болгон анализаторлордун үстүндө изилдөө жүргүзүп төмөнкү проблемага туш келдик.

- Веб трафик отчетунун бир нече убакыт кечигүүсү (лог файлдын көлөмүнүн чоңдугунан көбүнчө лог-анализаторлор бир нече минутадан – бир нече саатка чейин иштеши мүмкүн).
- Веб-интерфейс жоктугу (Web-интерфейс аркылуу прокси сервердин жана анализатордун параметрлерин өзгөртүүгө мүмкүнчүлүк жок болгондуктан, түздөн түз конфигурациялык файлды билип, таап, өзгөртүү зарыл).
- Отчеттун сактоо жана башкаруу түрү (көб учурда жөнөкөй html-файл түрүндө сакталат, ошондуктан сактоодо чон ыңгайсыздыктарга алып келет.).
- Заматта (онлайн) мониторинг жүргүзүү мүмкүнчүлүгүнүн жоктугу.

Прокси сервердин лог файлы орточо 500 мегабайттан - 2 гигабайтга чейин өсүшү мүмкүн [1]. Кээбир чоң мекемелерде бир суткада 8-10 гигабайтка чейин лог файлдын өсүшү байкалат Бул лог файлды иштетүү үчүн анализаторлор бир нече саат талап кылат. Администраторлор анализаторду түнкү убакытка иштетип коюшат жана эртеси күнү гана маалыматты ала алышат жана заматта (онлайн) трафик жөнүндө маалымат алуу кыйынчылыгына алып келет. Бул проблеманы cron-утилитасы жардамы менен анализаторду ар бир минута сайын чакыруу менен чечүүгө аракет жазашат. Учурдагы иштин максаты бар болгон SQUID прокси серверинин анализаторлорун изилдөө жана жаралган кыйынчылыктардын эффективдүү чечүү жолун табуу.

---

[1] www.entensys.com
[2] http://www.labris.eu
[3] www.squid-cache.org
[4] http://sarg.sourceforge.net

Төмөнкү таблицада SQUID тин жараткан лог файлын анализдөөчү программалардын тизмеси жана кыскача өзгөчөлүктөрү көрсөтүлгөн.

1-Таблица

Аты	БД	Прог.тили	ОС	Шилтеме
Free SA	**Жок**	C/PHP	Linux, Unix	http://sourceforge.net/projects/free-sa/files/
LightSquid	**Жок**	Perl	Linux, Unix	http://lightsquid.sourceforge.net/
ProxyStat	**Жок**	Perl	Linux, Unix	-
MySAR	MySQL	PHP/C++	Linux, Unix	http:// giannis.stoilis.gr/software/**mysar**/
SAMS	MySQL	C++	Linux, Unix	http://sams.perm.ru/
SARG	**Жок**	C	Linux, Unix	http://sarg.sourceforge.net/
Squid Traffic Counter	**Жок**	Sh, Perl, CGI	Linux, Unix	http://stc.nixdev.org
Squid2MySQL	MySQL	PHP	Linux, Unix	http://evc.fromru.com/squid2mysql/index.html
SquidGuard	**Жок**	C	Linux, Unix	http://www.squidguard.org/
Squid-PB	MySQL	PHP	Linux, Unix	http://pb.pils.ru/
Statman	PostreSQL	Perl	Linux, Unix	http://cyberos.narod.ru/statman/index.html

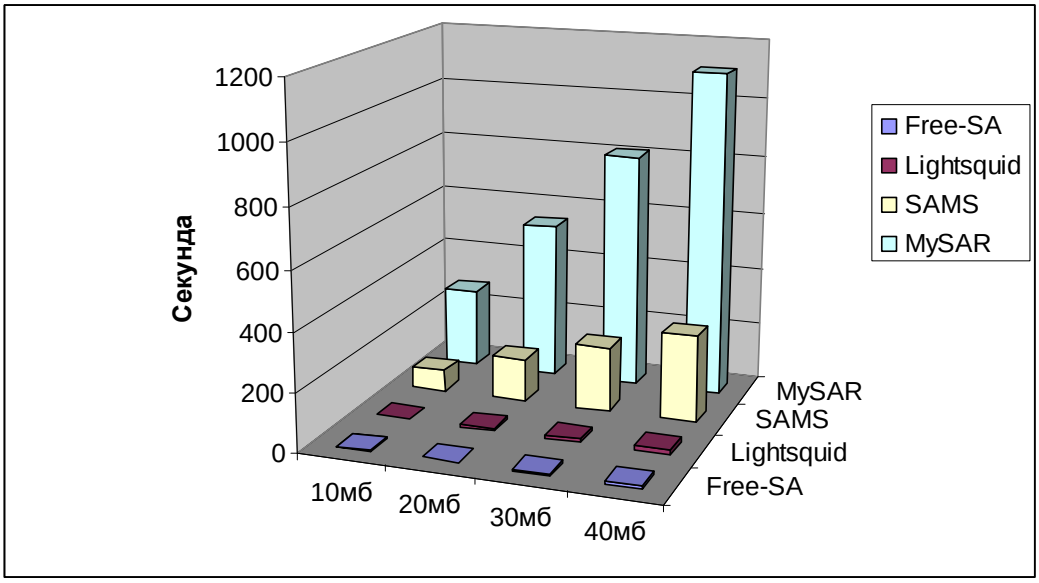
Бул жерде эң популярдуу жана кеңири таралган анализаторлор булар LightSquid, FreeSA, SAMS, MySAR. Булардын баардыгы «GNU General Public License»[5] лицензиясы менен эркин таркатылат. Бул үч анализаторлор бир системага[6] орнотулуп, жана иштөө убактысы боюнча салыштырылып төмөнкү жыйынтыка жетиштик. (2-Таблица жана 1-График)

2-Таблица

	Access.log файлдын көлөмү			
	10Mb	20Mb	30Mb	40Mb
Free-SA	2,21 сек	4,79 сек	7,03 сек	10,72 сек
Lightsquid	3,6 сек	7,61 сек	10,76 сек	14,73 сек
SAMS	73,18 сек	148,81 сек	223,43 сек	298,45 сек
MySAR	273,57сек	538,17 сек	808,36 сек	1113.11 сек

1-График

[5] http://www.gnu.org/copyleft/gpl.html
[6] FreeBSD 8.0 RELEASE, Squid Cache 2.7 STABLE7, MySQL 5.0.86, Apache 2.2.13, GCC 4.2.1, PHP 5.2.11, Perl 5.8.9



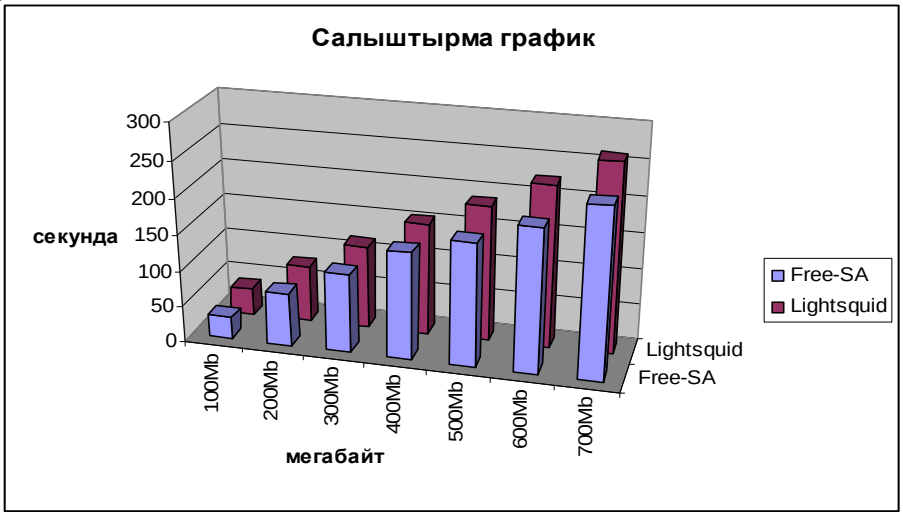
Көрүнүп тургандай SAMS жана MySAR абдан жай иштөөдө, себеби SAMS жана MySAR баардык маалыматты берилиштер базасында сакташат. Ошондуктан лог файлды анализдөөдө убакыт боюнча Free-SA жана Lightsquid тен абдан артта калышкан. Бирок SAMS жана MySAR тарабынан түзүлгөн БД-да сакталган маалымат үстүндө кошумча амал жүргүзүү мүмкүн. Ошондой эле SAMS тын абдан ыңгайлуу Web-интерфейси бар. Ушул өзгөчүлүгү үчүн SAMS популярдуу болуп келе жатат.

SAMS жана MySAR иштөө убакыты боюнча абдан артта калган үчүн кийнки тестерде катышка алынган жок. Ал эми төмөнкү таблица боюнча Free-SA анализатору access.log файлы чоңойгон сайын Lightsquid-тен батыраак иштеши көрүнүп турат. (3-Таблица жана 2-График).

3-Таблица

	Access.log файлдын көлөмү						
	100Mb	200Mb	300Mb	400Mb	500Mb	600Mb	700Mb
Free-SA	30,6 сек	73,37 сек	109,17 сек	147,91 сек	169,75 сек	197,3 сек	233,68 сек
Lightsquid	34,73 сек	77,96 сек	115,33 сек	155,29 сек	188,31 сек	224,45 сек	262,33 сек
айырма	4,13	4,59	6,16	7,38	18,56	27,15	28,65

2-График.



Бул кубулуш Free-SA анализатору «C» тилинде, ал эми Lightsquid болсо

«Perl» тилинде жазылгандыгы үчүн байкалууда.

Изилдөөнүн негизинде бүгүнкү күндө бар болгон жана кеңири колдонулган Squid прокси сервердин анализаторлордун ичинен эң тез иштеген FreeSA болуп чыкты. Ал эми эң ыңгайлуу жана оңой тейлөө өзгөчүлүгү менен SAMS жеңип чыкты.

Access.log файлы чоң болгон сайын БД'ны колдонгон анализаторлор абдан ыңгайсыз болоору көрүнүктүү (SAMS, MySAR). Бул ыңгайсыздыкты cron утилитасы жардамы менен чечүү мүмкүн (мисалы анализатор ар 5 минута сайын иштетилип, access.log файлдын көлөмү кичине болуп турат).

Бирок эч бири жогоруда көрсөтүлүп кеткен проблемаларды толук түрдө чече албайт. Free-SA бат иштегени менен төмөнкү кемчиликтери бар:

- жыйнтык/отчет файл түрүндө сакталат;
- онлайн мониторинг өзгөчөлүгү жок (cron жардамы керек).

SAMS болсо

- абдан жай иштейт;
- онлайн мониторинг өзгөчүлүгү 10сек интервал менен иштейт.

Жыйнтык

Бул эки анализатордун өзгөчөлүктөрүн колдонуп, жана кошумча касиеттер менен толуктап, жаңы эффективдүү анализатор иштетилип чыгышы мүмкүн. Мисалы Squid2MySQL анализаторунда онлайн мониторинг жүргүзүү үчүн «access.log» файлы «pipe» каналы менен алмаштырылган. Бирок бул анализатордо кандайдыр убакыттан кийин «pipe» канал белгисиз себептердин негизинде катага учурап, баардык системаны кайрадан баштаганга алып келет.

Адабияттар:

1. «Squid: The Definitive Guide» By Duane Wessels. ISBN 0-596-00162-2. January, 2004.
2. «Linux Security Cookbook» By Daniel J. Barrett, Robert G. Byrnes, Richard Silverman. ISDN 0-596-00391-9. June, 2003.
3. www.squid-cache.org.
4. http://sourceforge.net/projects/free-sa/files/.
5. http://sams.perm.ru/.
6. http://lightsquid.sourceforge.net.