УДК 681.324

І.В. Кобзев[1], К.Е. Петров[1], Д.О. Руденко[2]

[1] *Харківський національний університет внутрішніх справ, Харків*
[2] *Харківський національний університет радіоелектроніки, Харків*

МЕТОДИ ВИЯВЛЕННЯ І ЗАСОБИ БОРОТЬБИ З ПЕРЕВАНТАЖЕННЯМ ЗОВНІШНІХ КАНАЛІВ ОРГАНІЗАЦІЇ НАДМІРНИМ МЕРЕЖНИМ ТРАФІКОМ

Стаття присвячена методам і інструментальним засобам контентної фільтрації міжмережного трафіку, що передається по протоколах прикладного рівня. Розглядаються програмні способи використання методів для створення систем фільтрації в глобальних і локальних мережах при передачі інформації.

Ключові слова: *пірінгові мережі, трафік, торрент, програмні засоби, аналіз.*

Вступ

Зростання кількості і обсягів ресурсів мережі Internet обумовлює необхідність пошуку нових ефективних методів для вирішення завдання обмеження доступу до ресурсів мережі, які є джерелом надмірного трафіку.

Надмірний об'єм широкомовного трафіку погано впливає на кінцеві станції, які визначають, чи потрібний їм цей трафік. Вживання заходів по виправленню або усуненню причин, які лежать в основі цього явища, може підвищити продуктивність роботи мережі і допоможе уникнути подальших проблем. Проте без відповідних інструментів і методів усунення несправностей ця робота може затягнутися надовго. До джерел небажаного або надмірного трафіку, по-перше, відносяться сторінки розважальних порталів, сайтів знайомств, пірінгових або Peer to Peer (P2P) застосувань, послуги ICQ або Skype. По-друге, існує ще декілька категорій сайтів: так звані «сайти для дорослих», екстремістські і інші сайти з сумнівним інформаційним змістом. Відвідування подібних сайтів співробітниками організацій в робочий час часто є прямим порушенням корпоративного регламенту, оскільки в результаті доступу до нецільової інформації витрачаються мережні ресурси (наприклад, трафік), а також робочий час співробітників організації. Крім того, багато розважальних сайтів сприяють розповсюдженню шкідливих програм (використовуючи вразливості Web-браузерів або пропонуючи користувачам посилання на «закачування» неперевіреного або неліцензійного програмного забезпечення).

Окрім цього при експлуатації корпоративної телекомунікаційної мережі можуть епізодично виникати ситуації порушення режиму нормального функціонування мережі, викликані перевантаженням каналів мережі, зокрема – зовнішнього. Вказані ситуації можуть спричинити відмову в роботі служб на окремих комп'ютерах, підмережах і мережі в цілому. Часто такі перевантаження не є наслідком навмисної атаки на мережу або вірусної активності, а виникають при роботі на деяких комп'ютерах тих або інших мережних застосувань, що створюють надмірне навантаження на канали мережі. При цьому причину нестабільної роботи мережі досить важко діагностувати.

Відзначимо, що досить часто застосування, які створюють аномальне навантаження на канали, є «непрофільними» для корпоративної мережі. Вони не використовуються для вирішення тих або інших інформаційно-обчислювальних задач власника мережі. Тому завдання виявлення факту наявності непрофільного трафіку, а також комп'ютерів, які є джерелами або споживачами вказаного трафіку – вельми актуальне. Шляхом обмеження мережної активності таких комп'ютерів технічними або адміністративними заходами можливе виключення аномального завантаження каналів трафіком цих комп'ютерів.

Пірінгові мережі, як основне джерело надмірного трафіку

Торрент, як і багато інших пірінгових мереж, повністю заблокувати непросто: концепція цієї технології така, що за бажанням можна скористатися масою обхідних маневрів і маленьких хитрощів, що дозволяють обійти як прямі, так і непрямі заборони.

На сьогоднішній день можна назвати лише ряд напівзаходів, розрахованих на те, що торрент-клієнти не підтримують той або інший сценарій роботи. Наприклад, можна вимагати, щоб будь-який мережний трафік був аутентифікований, але цей спосіб придатний лише для крупних організацій з розвиненою мережною інфраструктурою. Дещо простіше встановити проксі-сервер і вимагати від користувачів працювати лише через нього, проте напевно знайдуться варіанти обходу цієї заборони. В цьому випадку можна як мінімум заборонити тор-

рент-клієнти по рядку user-agent через http-запит або через іншу оригінальну для конкретного торрент-трафіку сигнатуру [1].

Взагалі, розглядаючи можливі методи блокування небажаного трафіку, можна виділити два ключові підходи: індивідуальний (для кожного робочого місця) і груповий, або мережний (для всіх користувачів). Перший придатний при невеликій кількості ПК і передбачає встановлення засобів контролю на кожен комп'ютер окремо. У перелік таких засобів входять брандмауери, що дозволяють заблокувати паролем доступ до налаштувань: з їх допомогою забороняється як запуск так і робота з мережею певним застосуванням, так і використання специфічних портів (в ідеалі залишається відкритим лише необхідний мінімум) у поєднанні з забороною користувачеві встановлювати власні програми, що знову-таки легко обходиться. Крім того, встановлюються засоби контролю, моніторингу і видаленого управління, які автоматично повідомляють адміністратора про активізацію невпізнаного застосування або перевищення квоти на мережевий трафік. Не варто забувати і про персональні засоби доступу: підключення до локальної мережі таких пристроїв, як смартфони, планшети, ноутбуки і подібні до них повинно мати жорстко регламентований характер.

Для великої кількості робочих місць простіше застосувати глобальні (централізовані) методи, серед яких за найбільш просте і дієве вважається блокування специфічних портів. На жаль, і це не панацея: досвідчені користувачі знайдуть спосіб перенаправити потоки на інші порти, але деяка частина менш технічно підготовлених порушників не зможе перевантажувати трафік. Другим варіантом є перенаправлення зовнішніх запитів на проксі-сервер, а також проходження їх через стандартний шлюз і брандмауер, в яких повинно бути реалізовано усі можливі методи захисту: блокування портів (відкриття лише дозволених), аутентифікація трафіку (з подальшою забороною недозволеного application/x-bittorrent), обмеження кількості потоків, що формуються кожним комп'ютером в мережі тощо.

До речі, остання міра, поряд з шейпінгом (обмеженням) трафіку, якщо і не припинить доступ до торрент-сервісів, то зробить його марним: викачування навіть невеликого Mp3-файла може затягнутися на добу, що рано чи пізно змусить порушника відмовитися від використання пірінгового клієнта на робочому місці.

Як додатковий засіб можна застосувати мережні сніффери і з їх допомогою відстежувати (вручну або автоматично) робочі місця, на яких використовуються пірінгові клієнти. Природно, з подальшим використанням як адміністративних, так і технічних заходів.

Будь-яку дію породжує протидія, і нерідко пірінгові мережі вельми показові як джерело «конфліктного» контенту в правовому плані. Піратське програмне забезпечення, незаконні відео і аудіо матеріали, інша інформація, отримана за допомогою P2P-технологій, не просто аморальні, але і ставлять організацію, в якій подібне порушення допускається, в один ряд з порушниками закону: адже основний принцип торрент-мереж – «викачав сам, віддай іншому».

Методи аналізу трафіку

Існуючі системи обмеження доступу до мережних ресурсів мають можливість перевіряти на відповідність заданим обмеженням не лише окремі пакети, але і їх зміст. В даний час в системах контентної фільтрації застосовуються наступні методи фільтрації Web-контенту: на ім'я DNS або конкретної IP-адреси, за ключовими словами усереднені Web-контенту і за типом файлу. Щоб блокувати доступ до певного Web-вузла або групи вузлів, необхідно задати безліч URL, контент яких є небажаним.

URL-фільтрація забезпечує ретельний контроль безпеки мережі. Однак не можна передбачити наперед всі можливі неприйнятні URL-адреси. Крім того, деякі Web-вузли з сумнівним інформаційним наповненням працюють не з URL, а виключно з IP-адресами.

Виявлення непрофільного трафіку може виконуватись з використанням засобів класифікації мережевого трафіку за типами додатків, що генерують цей трафік. Методи аналізу змісту пакетів можна розділити за місцем знаходження сигнатури: в заголовках мережевого, транспортного або прикладного рівнів або в корисному навантаженню пакету.

Аналіз сигнатури являє собою перевірку відповідності налаштувань системи і активності користувача з базою даних відомих атак та вразливостей системи. Більшість комерційних продуктів виявлення атак проводять аналіз сигнатур в порівнянні з базою даних відомих атак, що постачається продавцем. Додаткові сигнатури, встановлені клієнтом, також можуть бути додані як частина процесу конфігурації системи виявлення атак [2].

Найбільш поширеним методом цього типу є метод ідентифікації прикладного протоколу за відомим номером використовуваного ним порту [3]. Цей метод має як явні переваги, так і певні недоліки. Основною перевагою методу є його «швидкодія». У той же час точність класифікації всупереч інтуїтивним очікуванням найчастіше виявляється невисокою. Це пов'язано з тим, що деякі мережні додатки «маскуються» від розпізнавання цим методом шляхом використання портів, які стандартно використовуються іншими широко відомими застосуваннями. Загальним недоліком усіх сигнатурних методів є складність розширення набору сигнатур при виявленні того, що використовуваний набір не забезпечує розпізнавання деякого нового класу трафіку.

Для виконання такого розширення потрібні досить великі трудовитрати кваліфікованих фахівців.

Методи другого типу засновані на використанні статистичного аналізу трафіку мережевих з'єднань. Ці методи, в свою чергу, поділяються на методи аналізу особливостей поведінки вузлів мережі і засновані на аналізі особливостей інформаційних потоків між мережевими додатками. Всі різновиди, що засновані на методах класифікації трафіку, вимагають їх попереднього «навчання» на заздалегідь підготовлених даних. Найчастіше використовується інформація транспортного рівня про взаємодію між пристроями, які підключені до комп'ютерної мережі.

До достоїнств методів зазначеного типу відноситься можливість розпізнавання шифрованих даних, оскільки беруться до уваги саме особливості поведінки трафіку в потоці, а не зміст пакетів. Крім того, забезпечується можливість розпізнавання аномального трафіку не передбаченого заздалегідь класу.

До основних недоліків цих методів відносяться неможливість безпомилкової ідентифікації трафіку конкретних мережевих додатків і дуже висока обчислювальна складність, викликана необхідністю аналізу всього потоку, а не декількох перших пакетів в потоці [2].

За результатами аналізу розглянутих методів і засобів класифікації трафіку далі буде запропоновано методи обмеження трафіку мережевих додатків.

Програмні засоби контролю трафіка і управління доступом до мережі

Існують декілька способів заборони доступу на певні сайти. Розглянемо кожен з них детальніше.

Найпростіший спосіб – це створення фіктивного DNS-запису. На комп'ютері, звідки здійснюється доступ в Internet, редагується текстовий файл hosts, який знаходиться в папці c:\windows\system32\drivers\etc\, що містить список DNS-імен сайтів, до яких закривається доступ. Наприклад:

www.rutor.org 127.0.0.1;

www.ex.ua 127.0.0.1.

Тепер, при зверненні до сайту www.rutor.org (торрент-трекер) браузер не зможе знайти IP-адрес для імені www.rutor.org, а отже і відкрити цей сайт. Недолік даного методу в тому, що такий механізм діє лише для одного комп'ютера. Якщо в мережі декілька комп'ютерів, то на кожному комп'ютері потрібно відредагувати файл hosts. Крім того, якщо сайт має декілька дзеркал, то кожне таке дзеркало вимагає окремого запису у файлі hosts.

Також адміністратор мережі може використовувати налаштування проксі-сервера. Суть даної технології полягає в налаштуванні програмного забезпечення проксі-сервера (наприклад, Squid або SquidNt), в якому створюються "чорні списки" сайтів, що закриті для відвідування. Використання проксі-сервера дозволяє гнучко вказати небажані слова в закритих сайтах. Мінус цього методу – в необхідності примусового налаштування браузерів клієнтських комп'ютерів на використання проксі-сервера. Крім того, необхідно передбачити, щоб користувачі не користувалися Internet в обхід проксі-сервера та не використовували анонімні проксі-сервери.

Окрім вищесказаного можна використовувати спеціальні програмні засоби.

TMeter. Ця програма використовує технологію URL-фільтрації сайтів. Суть технології URL-фільтрації – в безпосередньому аналізі вмісту кожного мережевого пакету. Якщо в мережевому пакеті знайдений заголовок Web-запиту, що містить адресу Web-сайту, до якого відбувається запит і його необхідно заблокувати, то програма TMeter виконує такі дії:

— блокує мережевий пакет із запитом клієнта до Web-сервера;

— посилає клієнтові відповідь "як би від імені Web-сервера", що містить сторінку "Доступ заблокований";

— коректно закриває TCP-з'єднання, відповідаючи клієнтові і Web-серверу пакетами з прапорами FIN.

Таким чином, URL-фільтр може заблокувати будь-який сайт по масці імені (заблокувати всі піддомени певного домена), заблокувати завантаження файлів по їх розширенню, наприклад *.mp3, *.ogg, *.wma, *.avi, *.mpg, *.wmv, *.mpg і створити "білий список" дозволених сайтів; доступ до решти всіх сайтів заблокувати [4].

Lan2net NAT Firewall – програмний міжмережевий екран, призначений для організації безпечного доступу в Internet з функціями захисту мережі, фільтрації сайтів, контролю і обліку трафіку. Його розробкою займається російська компанія Нетсиб, що має, до речі, статус Microsoft Small Business Specialist.

Можливостей в продукту Lan2net дуже багато. Нас же цікавить функція блокування доступу до сайтів, яка реалізується за рахунок використання механізму фільтрації сайтів по URL і IP. Заборонити доступ по IP можна при створенні правила firewall або правила для групи [5].

Kerio Winroute. У сучасних мережах для організації спільного доступу в Internet і захисту внутрішньої мережі часто використовується Kerio WinRoute, що вміє блокувати будь-який трафік, визначений адміністратором системи. До складу продукту включений цілий ряд компонентів: файервол з функціями NAT, проксі і VPN-сервер, антивірусний модуль, розподіл навантаження, блокування P2P-трафика і багато іншого. У програмі включено декілька компонентів, за допомогою яких задаються політики, що дозволяють блокувати доступ до певних URL по протоколах HTTP і FTP на підставі шаблону. Шаблон адреси можна задати прямо в прави-

лі фільтрації, але це незручно. За наявності декількох шаблонів, до яких необхідно застосувати одну дію, доведеться додавати декілька правил, що ще більш ускладнює процес. Враховуючи, що адміністратор системи навіть для невеликої мережі формує велику кількість правил, доведеться довго шукати потрібне, якщо знадобиться щось змінити.

SurfAnalyzer. Дане спеціалізоване рішення дозволяє блокувати доступ до небажаних ресурсів, які відволікають від роботи або несуть потенційну небезпеку. Програма, яка є посередником між Internet і користувачем, пропускає через себе весь трафік, тому з її допомогою дуже просто контролювати закачування файлів з певними розширеннями (.exe, .com, .zip та ін.), вкладення в електронній пошті, фільтрувати IM-повідомлення, блокувати деякі типі сайтів [7].

BitTally. Програма обліку трафіку надає користувачеві зведення про Web-сервер-серфінг в розрізі користувачів, доменів і категорій доменів по країнах. Програма формує звіти про трафік з розбиттям по користувачах і групах користувачів, протоколах і групах протоколів, мережах призначення і країнах – облік трафіку ведеться з автоматичним визначенням всіх цих даних.

Програма попереджає адміністратора мережі про тривале використання певного протоколу, розсилку спаму, різку зміну об'єму трафіку, небажані пошукові запити. BitTally може автоматично заблокувати неприйнятний Web-контент, P2P або будь-які інші протоколи. При цьому можлива фільтрація по іменам або групам користувачів, часу доби, дням тижня, конкретним протоколам або групам протоколів, мережам, доменам або категоріям доменів, країнам [8].

Блокування трафіку через iptables

Не дивлячись на те, що можна створити декілька різних політик IP-безпеки, не можливо призначити одночасно більш чим одну політику. Але в рамках однієї політики є можливість створювати скільки завгодно фільтрів для різних випадків, і активувати їх при необхідності установкою або зняттям відповідного прапорця в списку.

Такий спосіб блокування не найшвидший в налаштуванні і не найзручніший. Але він завжди працює, незалежно від наявності файерволу в системі. Що ще важливо, політика блокування діє для всіх програм. Якщо ви, наприклад, заблокували рекламні сайти через політику IP-безпеки, то не побачите реклами у всіх браузерах, а не лише там, де встановлена банерорізка. Ще один великий плюс полягає в тому, що для блокування доступу до окремих ресурсів не вносяться зміни в системні файли.

Таким чином, один з найкращих способів блокування ботів, це блокування через iptables.

Найбільш поширений варіант використання послуг iptables і squid + squidguard. Можна ще додати HAVP (HTTP проксі-антивірус) + ClamAV (антивірус-сканер) для фільтрації трафіку на віруси. Закриваються всі порти в iptables, окрім необхідних (80, 25, 110, 443), а http-протокол фільтрується безпосередньо на проксі-сервері (squid). Використання такого методу, по-перше, унеможливлює створення правил для кожного сайту окремо, а по-друге, навантаження на проксі-сервер в рази менше, ніж при використанні htaccess фільтрації.

Всі клієнти ICQ для підключення до сервера за умовчанням використовують адресу login.icq.com і порт 5190. У рекомендаціях по використанню ICQ сказано, що в разі недоступності 5190 підключитися можна і до порту 443.

```
$ host login.icq.com
login.icq.com is an alias for login.messaging.aol.com
login.messaging.aol.com has address 64.12.172.97
```

Приклад показує, що login.icq.com є псевдонімом для іншого імені, і, можливо далеко не єдиним. Його також потрібно заблокувати в правилах. Ситуацію з ICQ і багатьма іншими сервісами трохи ускладнює наявність великої кількості псевдонімів і підсервісів, тому доводиться шукати і закривати всі можливі варіанти використання цього мережного протоколу. Команда dig надає повну інформацію про будь-який домен (dig login.icq.com).

У першому випадку заблокувати доступ дуже просто. Спочатку робиться обмеження по порту і потім додається правило для домену.

```
iptables -A FORWARD -p TCP --dport 5190 -j DROP
iptables -A OUTPUT -d login.icq.com -j REJECT
```

Використання доменного імені з одного боку більш універсально, оскільки IP завжди може змінитися, але з іншого боку необхідно блокувати трафік і по IP-адресу. Тим більше, розробники постійно йдуть назустріч клієнтові і пропонують сервіси подібно www.icq.com/icq2go, що дозволяють спілкуватися через Web-інтерфейс. Хоча саме цей варіант легко блокується – досить закрити доступ до діапазону IP (він видно у виведенні dig):

```
iptables -A OUTPUT -d 64.12.0.0/8 -j REJECT
iptables -A OUTPUT -d 205.188.0.0/24 -j REJECT
```

Окрім цього альтернативні служби ICQ такі як:

Yahoo! Messenger використовує TCP-порти: 5000-5001,5050,5100 і UDP-порти: 5000-5010;

MSN – 1863;

Jabber/Gtalk - 5222, 5223;

IRC зазвичай використовує 6667-6669;

Mail-агентпрацює по портах: 2041, 2042.

Правила для цих мереж будуються по аналогії з попереднім. Наприклад, для Yahoo Messenger це робиться таким чином.

```
iptables -A FORWARD -p TCP --dport 5000:5001
```

-j REJECTiptables -A FORWARD -p TCP --dport 5050 -j REJECT

iptables -A FORWARD -p TCP --dport 5100 -j REJECT

iptables -A FORWARD -p UDP --dport 5000:5010 -j REJECT

iptables -A FORWARD -d cs.yahoo.com -j REJECT

iptables -A FORWARD -d scsa.yahoo.com -j REJECT

Щоб обмежити доступ до пірінгових мереж, найпростіший спосіб закрити програмні порти для доступу до цих мереж. Наприклад, EMULE використовує порти 4661-4711, а Торрент 6881-6999.

Щоб заблокувати всі вхідні запити порту 6881 необхідно зробити наступне:

iptables -A INPUT -p tcp --dport 6881 -j DROP

iptables -A INPUT -i eth1 -p tcp --dport 6881 -j DROP.

Щоб заблокувати певний домен необхідно взнати його IP-адресу:

host -ta www.thepiratebay.se

www.thepiratebay.se has address 194.71.107.15.

Знайдемо CIDR для 194.71.107.15:

whois 194.71.107.15 grep CIDR

CIDR: 194.71.107.15/24.

Заблокуємо доступ на 194.71.107.15/24:

iptables -A OUTPUT -p tcp -d 194.71.107.15/24 -j DROP.

Також можна використовувати домен для блокування:

iptables -A OUTPUT -p tcp -d www.thepiratebay.se -j DROP

iptables -A OUTPUT -p tcp -d www.thepiratebay.se -j DROP

Висновки

В зв'язку з широким використанням Internet при ведені бізнесу та у повсякденному житті з'явилася гостра необхідність заборонити співробітникам організацій доступ до небажаних сайтів, оскільки використання робочого часу і ресурсів значно зменшує продуктивність праці. Пірінгові та широкомовні протоколи цілеспрямовано обходять мережні політики безпеки і збільшують інформаційні ризики організацій.

Від використання пірінгових мереж виграють лише ті приватні особи або організації, які поширюють матеріали в мережі Internet. Для решти користувачів P2P-мережі та їх аналоги створюють лише проблеми, оскільки «забруднюють» канали зв'язку величезними об'ємами даних.

В статті розглянуті лише основні параметри, що дозволяють налаштувати доступ до Internet і приділили основну увагу фільтрації небажаного та широкомовного мережевого трафіку.

Список літератури

1. Как закрыть торренты в организации / [Електронний ресурс]. – Режим доступу URL: http://www.it-world.ru/tech4human/solutions/7311.html.

2. Обнаружение атак и анализ защищенности: технические концепции и определения / [Електронний ресурс]. – Режим доступу URL: http://bugtraq.ru/library/books/icsa/chapter6/?k=9.

3. Содержимое пакетов. Безопасность компьютерных сетей / [Електронний ресурс]. – Режим доступу URL: http://bezopasnieseti.ru/soderzhimoe-paketov/soderzhimoe-paketov.html.

4. TMeter / [Електронний ресурс]. – Режим доступу URL: http://www.tadviser.ru/index.php/Продукт:TMeter.

5. Lan2net Firewall 3 – программный firewall, предназначенный для организации безопасного доступа в Интернет, защиты сети, фильтрации сайтов, контроля и учета трафика / [Електронний ресурс]. – Режим доступу URL: http://www.lan2net.ru/

6. Обзор Kerio WinRoute Firewall - файрвола для защиты сетей предприятий малого и среднего бизнеса / [Електронний ресурс]. – Режим доступу URL: http://www.ixbt.com/soft/kerio-winroute-firewall.shtml.

7. Софт обзор / obzorpo.ru новости ПО web индустрии / [Електронний ресурс]. – Режим доступу URL: http://www.obzorpo.ru/internet-soft/servernoe-po/ surfanalyzer-1.3.html

8. Программа учета трафика. Подробное описание [Електронний ресурс]. – Режим доступу URL: http://www.bittally.ru/details.

Надійшла до редколегії 8.02.2013

Рецензент: д-р техн. наук, проф. С.Г. Удовенко, Харківський національний університет радіоелектроніки, Харків.

МЕТОДЫ ОБНАРУЖЕНИЯ И СРЕДСТВА БОРЬБЫ С ПЕРЕГРУЗКОЙ ВНЕШНИХ КАНАЛОВ ОРГАНИЗАЦИИ ИЗБЫТОЧНЫМ СЕТЕВЫМ ТРАФИКОМ

И.В. Кобзев, К.Э. Петров, Д.А. Руденко

Статья посвящена методам и инструментальным средствам контентной фильтрации межсетевого трафика, который передается по протоколам прикладного уровня. Рассматриваются программные способы использования методов для создания систем фильтрации в глобальных и локальных сетях при передаче информации.

Ключевые слова: *пиринговые сети, трафик, торрент, программные средства, анализ.*

METHODS OF DETECTION AND MEAN OF FIGHT AGAINST THE OVERLOAD EXTERNAL CHANNELS OF ORGANIZATION A SURPLUS NETWORK TRAFFIC

I.V. Kobzev, K.E. Petrov, D.A. Rudenko

The article is devoted methods and tools of content filtration of internetworking traffic which is passed on protocols of application layer. The programmatic methods using methods are examined for creation systems for filtration in global and local networks at an information transfer.

Keywords: *peer networks, traffic, torrent, programmatic facilities, analysis.*