УДК 004.057.4

Даценко І.Ю.,
Дегтярьова Л.М., к.т.н., доцент,
Полтавський національний технічний
університет імені Юрія Кондратюка

ПРИНЦИПИ ОРГАНІЗАЦІЇ ОБЛІКУ IP-ТРАФІКУ У МЕРЕЖАХ ДЛЯ ОС WINDOWS

***Анотація**. В статті приведено необхідність контролю інформаційних потоків і здійснення обліку трафіку між корпоративною мережею і Інтернет-трафіком, принципи організації обліку IP-трафіку, принципи та методи збору інформації про трафік. IP-пакет не копіюється, а пересилається в програмне забезпечення для аналізу, здійснюється зворотний зв'язок з пристроєм доступу, застосовуючи інтелектуальні алгоритми обмеження доступу для окремих клієнтів, протоколів та ін.*

***Ключові слова:** трафік, інтернет, мережа, програма, логістика, інформація, потік, моніторинг*

Вступ

У час високих технологій з'явилася ще одна видаткова графа - Інтернет. Однак, щоб мати достовірні дані про розміри платежів, необхідно щомісяця враховувати використовуваний трафік інтернету. Застосування систем обліку і тарифікації послуг з доступу до інтернету є необхідною мірою, адже неконтрольований доступ до виділеного каналу може приносити непрямі збитки, у зв'язку з перевантаженням корпоративної локальної мережі та зловживаннями, пов'язаними з інтернетом. Спеціальні програми дозволяють задавати обмеження на кількість мегабайтів, завантажених в один з двох

звітних періодів: добовий та місячний. Таким чином, адміністратор може обмежувати обсяг інформації, що завантажується. При аналізі значень обчислюється поточна швидкість передачі даних, динаміка змін яка відображається у вигляді графіка. Крім цього, отримана статистика зберігається у файли і на її основі формуються різні звіти і діаграми. В процесі обліку трафіку проводиться моніторинг за встановленими критичними значеннями швидкості і обсягом трафіку.

Необхідність контролю інформаційних потоків та обліку трафіку між корпоративною мережею і Інтернет-трафіку

Якщо мова йде про контроль трафіку, то слід зазначити, що зазвичай адміністрація компанії йде найбільш звичним та зручним шляхом - повністю накладає заборону на конкретні канали, наприклад соцмережі. Але експерти вважають, що такого роду контроль над трафіком не відрізняється особливою ефективністю. Управління матеріальним потоком неможливо здійснювати без обробки інформації, яка є його ініціатором, визначає його напрямок, інтенсивність, зміст, супроводжує його на всьому шляху руху.

Інформаційна логістика визначається як сфера діяльності, спрямована на організацію потоку даних, що супроводжують матеріальні потоки, за допомогою створення та управління інформаційними системами, які технічно і програмно забезпечують передачу і обробку логістичної інформації. Отже основним завданням інформаційної логістики є забезпечення високого ступеня наповнення інформацією системи управління, а також надання кожному рівню ієрархії управління логістичної системи необхідної йому інформації належної якості і в необхідні терміни.

Значення інформаційного забезпечення логістичного процесу настільки важливе, що багато фахівців виділяють особливу інформаційну логістику, яка має самостійне значення в бізнесі та управлінні інформаційними потоками і ресурсами. Інформація виступає рушієм діяльності логістичної системи і

дозволяє їй пристосовуватися до нових умов. У зв'язку з цим одним із ключових понять логістики є поняття інформаційного потоку. Матеріальні потоки обов'язково супроводжуються інформаційними потоками.

Інформаційні потоки класифікуються за різними ознаками (табл. 1.).

Таблиця 1

Класифікація інформаційних потоків логістики

Ознака класифікації	Вид інформаційних потоків
Відношення до логістичної системи та її ланок	- внутрішні та зовнішні - горизонтальні і вертикальні - вхідні і вихідні
Вид носія інформації	паперові, на магнітних носіях, електронні
Періодичність надання інформації	регулярні, періодичні, оперативні
Призначення інформації	директивні, нормативно-довідкові, обліково-аналітичні, допоміжні
Ступінь відкритості	відкриті, закриті, секретні
Спосіб надання	кур'єрські, поштові, телеграфні; телефонні, факсові, радіотелевізійні, електронна пошта, телекомунікаційні, інтернетівські

Інформація полегшує координацію та планування щоденних операцій, а також контроль над ними. Як правило, зміст інформаційного потоку відображує зміст матеріального. Недостовірна та неоперативна інформація або її відсутність можуть викликати перебої в логістичній системі та появу помилок різного рівня.

Інформаційна логістика вивчає інформаційні потоки і методи їхнього використання для логістичного управління. Застосування розроблених

інформаційною логістикою способів і методів оптимізації інформаційних потоків у практичній діяльності повинне забезпечити створення і функціонування інформаційних логістичних систем, керуючих виробництвом інформації, її рухом і доставкою споживачам з мінімальними витратами при максимальному задоволенні їхніх потреб в інформації.

Сучасні інформаційні системи дозволяють стежити за безперебійністю логістичних процесів у режимі реального часу, що дає можливість оперативно виявляти та управляти існуючими та потенційними збоями у трафіку потоків, виправляти їх, і тим самим підвищувати якість обслуговування споживачів.

Одним з основних завдань логістики є координація матеріальних і інформаційних потоків. Якісне інформаційне забезпечення логістичних процесів дозволяє заміняти запаси матеріальних і інших ресурсів надійною й оперативною інформацією.

Якісно спроектована корпоративна мережа характеризується визначеними і передбачуваними режимами потоків трафіку.

При визначенні способу проектування мережі важливо врахувати об’єм трафіку, який направляється у визначене місце, і найбільш розповсюджені джерела цього трафіку.

Контроль потоків трафіку в мережі оптимізує смугу пропускання і пропонує додатковий рівень безпеки за рахунок моніторингу. Розуміння режимів і потоків трафіку дозволяє мережевому адміністратору прогнозувати очікувані об’єми і типи трафіку. При виявленні несподіваного трафіку в мережі виконується фільтрація цього трафіку та аналіз його джерела.

При визначенні механізму керування мережевим трафіком важливо розуміти тип трафіку, що передається через мережу, а також текучі потоки трафіку. Якщо типи трафіку невідомі, для перехоплення й аналізу трафіку можна скористатися перехоплювачем пакетів.

Використовуючи дані, отримані від перехоплювача пакетів, адміністратори можуть визначити потоки трафіку. Вони аналізують ці дані по джерелу, призначенню і типу переданого трафіку. Результати аналізу можна

використовувати при прийнятті рішень про ефективне керування трафіком. Цього можна досягти шляхом зменшення непотрібних потоків трафіку чи зміни режиму потоків за рахунок переміщення сервера.

Принципи організації обліку IP-трафіку

Мережевий трафік або інтернет-трафік - обсяг інформації, переданої через комп'ютерну мережу за певний період часу.

Трафік підрозділяється на:

- вихідний (інформація, що надходить у зовнішню мережу);
- вхідний (інформація, що надходить із зовнішньої мережі);
- внутрішній (в межах певної мережі, найчастіше локальної);
- зовнішній (за межами певної мережі, найчастіше - інтернет-трафік).

Основну частину мережевого трафіку складають пакети з корисним навантаженням UDP і TCP - це протоколи 4-го рівня (L4). Крім адрес, заголовок цих двох протоколів містить номери портів, які визначають тип служби (додатки), що передає дані.

Для передачі IP-пакетів по проводах (або радіо) мережеві пристрої змушені «обертати» (інкапсулювати) його в пакет протоколу 2го рівня (L2). Самим поширеним протоколом такого типу є Ethernet. Фактична передача «провід» йде на 1м рівні. Зазвичай, пристрій доступу (маршрутизатор) не займається аналізом заголовків пакетів на рівні, вище 4го (виняток - інтелектуальні міжмережеві екрани).

Інформація з полів адрес портів, протоколів і лічильники довжин з L3 і L4 заголовків пакетів даних і складає той «вихідний матеріал», який використовується при обліку і управлінні трафіком. Власне обсяг переданої інформації знаходиться у полі Length (довжина пакету) заголовка IP (включаючи довжину заголовка). Через фрагментації пакетів внаслідок механізму MTU загальний обсяг переданих даних завжди більше розміру корисного навантаження.

Переважний обсяг трафіку структурований так, що складається з набору «діалогів» між зовнішніми і внутрішніми мережевими пристроями, так званих «потоків». Наприклад, у рамках однієї операції пересилання електронного листа (протокол SMTP) відкривається TCP-сесія між клієнтом і сервером. Вона характеризується постійним набором параметрів (IP-адресу джерела, TCP-порт джерела, IP-адресу одержувача TCP-порт одержувача). Замість того, щоб обробляти і зберігати інформацію попакетно, набагато зручніше зберігати параметри потоку (адреси і порти), а також додаткову інформацію — кількість і суму довжин переданих пакетів в кожну сторону, опціонально тривалість сесії, індекси інтерфейсів маршрутизатора, значення поля ToS та інше. Такий підхід вигідний для орієнтованих на з'єднання протоколів (TCP), де можна явно перехопити момент завершення сесії. Однак і для не орієнтованих на сесії протоколів можна проводити агрегацію і логічне завершення запису про потік, наприклад, таймауту.

Необхідно відзначити випадок, коли пристрій доступу здійснює трансляцію адрес (NAT, маскарадинг) для організації доступу в Інтернет комп'ютерів локальної мережі, використовуючи один, зовнішній, публічний IP-адрес. У цьому випадку спеціальний механізм здійснює підміну IP-адрес і TCP/UDP портів пакетів трафіку, замінюючи внутрішні (не маршрутизовані в Інтернеті) адреси відповідно до своєї динамічної таблиці трансляції. У такій конфігурації необхідно пам'ятати, що для коректного обліку даних по внутрішнім хостам мережі зняття статистики повинно здійснюватися способом і в тому місці, де результат трансляції ще не «знеособлює» внутрішні адреси.

Знімати і обробляти інформацію про прохідний трафік можна безпосередньо на самому пристрої доступу (ПК-маршрутизатор, VPN-сервер), з цього пристрою передаючи її на окремий сервер (NetFlow, SNMP), або «з дроту» (tap, SPAN).

Принципи та методи збору інформації про трафік

Головною проблемою при будь-якому моделюванні мережі є проблема збору даних про існуючу мережу. Збір даних про трафік при проектуванні мережі, що здійснюється за допомогою імітаційного моделювання, тобто включає в себе створення достовірної моделі, є необхідною умовою для створення такої моделі. Так як достовірна модель вимагає обов'язкової верифікації даних.

Існують різні методи і продукти для вирішення завдань збору даних про трафік, а завдання моніторингу і аналізу мережевого трафіку можуть вирішуватися на різних рівнях - починаючи від моніторингу завантаження мережевих інтерфейсів і закінчуючи аналізом пакетів, зібраних з критичних ділянок досліджуваної мережі.

В даний час широкого поширення набули методи, засновані на зборі та обробці деталізованої мережевої статистики. В цьому випадку безліч пакетних заголовків агрегується за схожими ознаками в так звані інформаційні записи, які в подальшому і є предметом аналізу. Такий підхід поєднує хорошу масштабованість з докладною інформацією про структуру потоків даних у досліджуваній мережі і дозволяє вирішувати цілий ряд завдань як дослідницького, так і адміністративного характеру.

Для того щоб будь-яка мережа передачі даних працювала якісно та безпечно вимагається вести статистику по трафіку і моніторити деякі параметри для наступного аналізу й оперативного управління мережею:

- IP адреса джерела, IP-адреса відправника;
- TCP/UDP порт джерела, TCP/UDP порт відправника;
- затримка (мін/макс/серед) - проміжок часу, необхідний для передачі пакета через мережу;
- джитер - затримка між двома послідовними пакетами;
- відсоток втрачених пакетів;
- обсяг трафіку, що передається в секунду (Мб/с);
- кількість IP-пакетів, що передаються в секунду;
- довжина IP-пакету (мін/макс/серед);

- виявлення та аналіз високорівневих прикладних протоколів.

Методи моніторингу засновані на маршрутизаторі - жорстко задані (вшиті) в маршрутизаторах та мають низьку гнучкість. Кожен метод розвивався багато років, перш ніж стати стандартизованим способом моніторингу.

SNMP - протокол прикладного рівня, який є частиною протоколу TCP/IP. Він дозволяє адміністраторам керувати продуктивністю мережі, знаходити і усувати мережеві проблеми, планувати зростання мережі. Протокол SNMP збирає статистику по трафіку до кінцевого хоста через пасивні датчики, які реалізуються разом з маршрутизатором.

Для протоколу SNMP притаманні три ключові компоненти: керовані пристрої (Managed Devices), агенти (Agents) та системи управління мережею (Network Management Systems - NMS).

Керовані пристрої включають в себе SNMP-агент і можуть складатися з маршрутизаторів, комутаторів, концентраторів, персональних комп'ютерів, принтерів і інших елементів, подібних цим. Вони несуть відповідальність за збір інформації і роблять її доступною для системи управління мережею (NMS).

Агенти включають в себе програмне забезпечення, яке володіє інформацією з управління, і переводять цю інформацію у форму, сумісну з SNMP. Вони закриті для пристрою управління.

SNMP - протокол рівня додатків, який використовує пасивні сенсори, щоб допомогти адміністратору простежити за мережевим трафіком і продуктивністю мережі. Хоча, SNMP може бути корисним інструментом для мережевого адміністратора, він створює можливість для загрози безпеці, тому що він позбавлений можливості аутентифікації. Він відрізняється від віддаленого моніторингу (RMON), тим, що RMON працює на мережному рівні і нижче, а не на прикладному.

RMON включає в себе різні мережеві монітори і консольні системи для зміни даних, отриманих у ході моніторингу мережі. Це розширення для SNMP інформаційної бази даних по управлінню. На відміну від SNMP, який повинен посилати запити про надання інформації, RMON може настроювати тони, які

будуть «моніторити» мережу, засновану на певному критерії. RMON надає адміністраторам можливість управляти локальними мережами також добре, як віддаленими від однієї певної локації/точки.

RMON, будується на протоколі SNMP. Хоча моніторинг трафіку може бути виконаний за допомогою цього методу, аналітичні дані про інформацію, отримані SNMP і RMON мають низьку продуктивність. Утиліта Netflow, яка обговорюється нижче, успішно працює з багатьма пакетами аналітичного програмного забезпечення, щоб зробити роботу адміністратора набагато простішою.

Netflow - це розширення, яке було представлено в маршрутизаторах Cisco, які надають можливість збирати IP мережевий трафік, якщо це вказано в інтерфейсі. Аналізуючи дані, які надаються Netflow, мережевий адміністратор може визначити такі речі як: джерело і приймач трафіку, клас сервісу, причини переповненості.

Перевага Netflow над іншими способами моніторингу, такими як SNMP і RMON, в тому, що в ній існують програмні пакети, призначені для різного аналізу трафіку, які існують для отримання даних від Netflow - пакетів і подання їх у більш доброзичливому для користувача вигляді.

Хоча технології, не вбудовані в маршрутизатор все ж обмежені в своїх можливостях, вони пропонують більшу гнучкість, ніж технології вбудовані в маршрутизатори. Ці методи класифікуються як активні і пасивні.

Активний моніторинг повідомляє проблеми в мережі, збираючи вимірювання між двома кінцевими точками. Система активного вимірювання має справу з такими метриками, як: корисність, маршрутизатори/маршрути, затримка пакетів, повтор пакетів, втрати пакетів, нестійка синхронізація між прибуттям, вимірювання пропускної здатності.

Пасивний моніторинг на відміну від активного не додає трафік в мережу і не змінює трафік, який вже існує в мережі. Також на відміну від активного моніторингу, пасивний збирає інформацію лише про одну точку в мережі.

Вимірювання відбувається набагато краще, ніж між двома точками, при активному моніторингу.

Комбінування активного та пасивного моніторингу - кращий спосіб, ніж використання першого або другого окремо. Об'єднані технології використовують кращі сторони і пасивного, і активного моніторингу середовищ.

WREN використовує комбінацію технік активного та пасивного моніторингу активно обробляючи дані, коли трафік малий, і пасивно обробляючи дані протягом часу великого трафіку. Він дивиться трафік і від джерела, і від одержувача, що робить можливим більш акуратні вимірювання. WREN використовує трасування пакетів від створеного додатком трафіку для вимірювання корисної пропускної здатності. WREN розбитий на два рівня: основний рівень швидкої обробки пакетів і аналізатор трасування користувальницького рівня.

Загалом, WREN - це дуже корисна установка, яка використовує переваги і активного, і пасивного моніторингу. Хоча ця технологія перебуває на ранньому етапі розвитку, WREN може надати адміністраторам корисні ресурси у моніторингу та аналізі їх мереж. Монітор власного конфігурування мережі (SCNM) - інший інструментарій, який використовує технології і активного, і пасивного моніторингу.

SCNM - це інструмент моніторингу, який використовує зв'язок пасивних і активних вимірювань для збору інформації на 3 рівні проникнення, вихідних маршрутизаторів, і інших важливих точок моніторингу мережі. Середа SCNM включає і апаратний і програмний компонент.

Підбираючи приватні інструменти для використання їх в моніторингу мережі, адміністратор повинен спочатку вирішити, чи хоче він використовувати добре зарекомендовані системи, які вже використовувалися багато років, або нові. Якщо існуючі системи більш відповідне рішення, тоді NetFlow - найбільш корисний інструмент для використання. Тим не менш, якщо адміністратор готовий спробувати нову систему, рішення комбінованого

моніторингу, такі як WREN або SCNM, - найкращий напрямок для подальшої роботи.

Висновок

З метою економії коштів на використання Інтернету, керівники компанії все частіше роблять вибір на користь безлімітних пакетів доступу до глобальної мережі. Але навіть при такому варіанті необхідність обліку витраченого трафіку залишається актуальною. Сьогодні облік трафіку може бути організований декількома способами в залежності від політики безпеки. Перш за все, можна використовувати протокол SNMP. Крім контролю споживаного трафіку на комп'ютерах під управлінням ОС Windows, програма здатна враховувати його і на різних мережевих пристроях, як комутатори, принтери тощо. Використання служби WMI як своєрідну альтернативу першим способом, дозволяє адміністратору встановити спеціальні агенти на віддалені машини. Також трафік може фіксуватися спеціальним протоколом NetFlow від компанії Cisco, який займається збором всієї необхідної інформації всередині мережі.

Посилання

1. Гаджинский А.М. Основы логистики: Учеб. пособие. – М.: ИВЦ «Маркетинг», 1996. – 124 с.

2. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы./ В. Г. Олифер, Н.А. Олифер. – М. : Питер, 2011. 944 с.

3. Остерлох Х. TCP/IP семейство протоколов передачи данных в сетях компютеров. / Х. Остерлох – М. : DiaSoft, 2002. – 576 с.

4. Танненбаум Э. Компьютерные сети./Э. Танненбаум – М. : Питер, 2009. 992 с.

5. Н.А. Олифер, В.Г. Олифер. Средства анализа и оптимизации локальных сетей. — Центр Информационных Технологий, 1998.

Authors:
Degtyaryova Larisa Nikolaevna, Datsenko Inna Yuriivna.

THE PRINCIPLES OF ORGANIZATION OF ACCOUNTING OF IP TRAFFIC IN NETWORKS FOR WINDOWS

Abstract. The article outlines the need to control information flows and implement traffic accounting between the corporate network and Internet traffic, the principles of organizing IP traffic accounting, principles and methods for collecting traffic information. The IP packet is not copied but forwarded to the software for analysis, feedback is made to the access device using intelligent access restriction algorithms for individual clients, protocols, and others..

Keywords: traffic, Internet, network, program, logistics, information, flow, monitoring.

Авторы:
Дегтярева Лариса Николаевна, Даценко Инна Юрьевна.

ПРИНЦИПЫ ОРГАНИЗАЦИИ УЧЕТА IP-ТРАФИКА В СЕТЯХ ДЛЯ ОС WINDOWS

Аннотация. В статье приведены необходимость контроля информационных потоков и осуществление учета трафика между корпоративной сетью и Интернет-трафиком, принципы организации учета IP-трафика, принципы и методы сбора информации о трафике. IP-пакет не копируется, а пересылается в программное обеспечение для анализа, осуществляется обратная связь с устройством доступа, используя интеллектуальные алгоритмы ограничения доступа для отдельных клиентов, протоколов и др..

Ключевые слова: трафик, интернет, сеть, программа, логистика, информация, поток, мониторинг.