УДК 004.72

Ю. Шилінська-Лобур, Т. Лобур
(Тернопільський національний технічний університет імені Івана Пулюя)

СИСТЕМА МЕРЕЖЕВОГО МОНІТОРИНГУ НА БАЗІ NETFLOW

Методи статистичного аналізу мережевого трафіку широко використовуються як інструменти прогнозування завантаженості каналів зв'язку, визначення втрат, якості надання послуг. Об'єктом аналізу, незалежно від архітектури мережі є мережевий трафік, оскільки інформація, яка передається в пакетах даних є джерелом всіх взаємодій.

Одним з інструментів моніторингу, що дозвляє проводити статистичну обробку є технологія Netflow. Протокол NetFlow розроблений компанією Cisco Systems і на даний час описаний в рекомендаціях RFC3334, RFC3954. Він дозволяє мереженим пристроям передавати дані про трафік, що проходить через даний пристрій, на будь-який вузол в мережі, де ці дані можуть накопичуватись, зберігатись в певному вигляді і відповідно відображуватися. Netflow надає можливість аналізу мережевого трафіку на рівні сеансів, створювати запис про кожну TCP/IP транзакцію. Система мереженого моніторингу на базі Netflow складається з трьох основних компонентів:

1. Сенсор.
2. Коллектор.
3. Система обробки і представлення даних.

Для збору статистики за допомогою Netflow необхідно налаштувати спеціальні netflow-сенсори, які збиратимуть інформацію з відповідних інтерфейсів і передаватимуть її netflow-колектору, який може розташовуватися локально або на окремому сервері. Інформацію, зібрану колектором, можна візуалізувати за допомогою графічного візуалізатора, або ж аналізувати за допомогою утиліт командного рядка. В якості сенсора можна використовувати доступні в стандартних UNIX-репозиторіях fprobe або softflowd.

Потоком для NetFlow вважається набір пакетів, які проходять в одному напрямі. Сенсор визначає, що потік закінчився за зміною параметрів пакетів, або за скиданням сесії TCP та відправляє інформацію до колектора. Залежно від налаштувань, сенсор також може періодично відправляти в колектор інформацію про активні потоки. Зібрана інформація зберігаєься у вигляді записів, що містять наступні параметри: номер версії протоколу; номер запису; вхідний і вихідний мережевий інтерфейс; час початку і кінця потоку; кількість байт і пакетів в потоці; адреса відправника і отримувача; порт джерела і призначення; номер протоколу IP; значення Type of Service; адреса шлюзу.

Система моніторингу Netflow забезпечує високу ефективність та дозволяє відслідковувати події, що відбувається в мережі у будь-який час і в будь-якому місці, отримувати інформацію в режимі реального часу, захищати мережу від внутрішніх і зовнішніх атак, зберігати статистичні дані і деталізацію вузлів, аналізувати мережеві потоки для ефективного планування потужностей і устаткування, швидко і точно усувати збої в роботі мережі, визначити аномалії, такі як DDOS-атаки, планувати і моніторити QoS політики, перевіряти піринг і SLA (Service Level Agreements), впровадити ip-заснований біллінг і облік, взнати, хто є найбільш активним користувачем і отримувати їх статистику. Завдяки використанню Netflow, система відрізняється високою гнучкістю і масштабованістю, легко розширювана і повністю сумісна з продуктами інших виробників.