УДК 004.75

Ладигіна О.А.
Центральноукраїнський національний технічний університет

Технологія CLEAR-Flow як компонент захисту віртуальної інфраструктури хмари

Сучасні технології віртуалізації в своєму складі містять компоненти захисту, але вони не здатні нейтралізувати весь спектр сучасних загроз, зокрема, несанкціонований доступ до інформації при її передачі по не перевірених каналах зв'язку, а також не можуть повністю виконати вимоги законодавства в галузі забезпечення інформаційної безпеки [1,2].

Для вирішення задач захисту віртуальної інфраструктури хмари і безпечного доступу до неї слід розробити стратегію з комплексним використанням технологій, які дозволять виконати всі вимоги в галузі забезпечення інформаційної безпеки.

В хмарі складно ідентифікувати легітимні запити і запити атаки. Оскільки хмарне середовище добре масштабується, то при DDoS-атаці служби використовують більше ресурсів протягом періоду атаки, щоб підтримати рівень SLA (угода про рівень обслуговування). DDoS-атаки можуть здійснюватися на мережевому рівні або на рівні додатків. При відображенні DDoS-атаки мережевого рівня, організатор атаки може перенести її на рівень додатків і створити більш складний тип DDoS-атак.

DDoS-атака полягає у скоординованій посилці величезної кількості помилкових запитів на ресурс, що атакуться, від безлічі комп'ютерів. В результаті атакований сервер витрачає всі свої ресурси на обслуговування цих запитів і стає практично недоступним для звичайних користувачів. Ситуація ускладнюється тим, що користувачі комп'ютерів, з яких направляються помилкові запити, можуть навіть не підозрювати про те, що їхні комп'ютери використовуються спеціальними троянами. Найчастіше зловмисники при проведенні DDoS-атак використовують трирівневу архітектуру. Простежити таку структуру в зворотному напрямку і виявити адресу вузла, який організував атаку, практично неможливо.

Так як хмара складається з декількох шарів - загальний захист системи дорівнює захисту найслабшої ланки. Для захисту від функціональних атак для кожного шару хмари необхідно створити стратегію захисту з використанням певних засобів захисту для: проксі - захист від DoS-атак; веб-серверу - контроль цілісності сторінок; серверу додатків - екран рівня додатків; шару системи управління базами даних - захист від SQL-ін'єкцій; системи зберігання - резервне копіювання і розмежування доступу.

Атаки на браузер є одним з найактуальнішими в даний час, тому що велика кількість клієнтів підключена до хмари через нього. Захистом від цих атак є сувора аутентифікація й використання шифрованого з'єднання з взаємною аутентифікацією, проте це не самі надійні засоби захисту, тому в цій галузі ще ведуться доопрацювання і пошуки оптимальних рішень.

Істотно підвищити інформаційну безпеку каналів зв'язку, контролюючи мережевий трафік і блокуючи мережеві аномалії, дозволяє технологія CLEAR-Flow [3].

CLEAR-Flow націлена на вирішення широкого набору груп задач:

- мережева безпека - виявлення вторгнень, запобігання поширенню мережевих вірусів, придушення атак типу DoS;
- мережеве управління - планування ємності, аналіз тенденцій, класифікація програм, реалізація алгоритмів гарантованої якості обслуговування;
- мережева тарифікація - облік трафіку і реалізація процедур,

необхідних для виконання угоди по рівню обслуговування.

Дана технологія за допомогою політик, перевіряє певний тип трафіку, дозволяючи комутатору вплинути на трафік, якщо перевищені певні критерії, а також може взаємодіяти зі сторонніми пристроями безпеки.

CLEAR-Flow знаменує собою новий підхід до управління вхідними та вихідними даними й вперше задачі моніторингу, аналізу та реагування реалізовані в рамках єдиного процесу в комутаційної матриці Ethernet. Базуючись на трьох основних групах процесів - моніторинг, аналіз та реагування - CLEAR-Flow реалізує повне рішення для виявлення подій і трендів в мережі, визначення їх впливу на її роботу і виконання відповідних дій для захисту.

Для моніторингу технологія CLEAR-Flow використовує можливості апаратної частини комутатора для сканування і фільтрації кожного пакету, який проходить через нього. При цьому відслідковуються тільки пакети, які відповідають критеріям моніторингу, заданими адміністратором. Пакети, що не представляють інтересу, система ігнорує. Якщо потрібне негайне реагування, апаратна частина комутатора інформує його програмну частину про необхідність зміни алгоритму обробки трафіку.

В системах, де вимоги до безпеки особливо високі, засоби CLEAR-Flow дозволяють відслідковувати керуючий трафік, направляти його на аналізатор і зберігати в архіві. Таким чином, можна виявляти атаки найвитонченіших хакерів, які і не підозрюють, що мережа здатна сама відслідковувати їх дії.

Для аналізу істинної природи підозрілого трафіку CLEAR-Flow дає на вибір один з трьох методів:

- дублювання трафіку - копія підозрілого трафіку дзеркально відбивається на один з портів комутатора і далі передається на аналізатор трафіку, де формується повна картина трафіку і можна максимально ретельно досліджувати пакети;

- дублювання через тунель - пакети забезпечуються додатковим заголовком IP і по тунелю направляються на віддалену систему для аналізу, що більш ефективно в великих мережах;

- SFlow - передача зовнішньому аналізатору тільки статистичних зразків трафіку, при цьому значно скорочується обсяг даних, що пересилаються, завдяки чому підвищується масштабованість процесу при великій кількості підозрілого трафіку.

У ситуації, коли класифікатор або зовнішній аналізатор виявить серйозну загрозу, буде перевищено встановлений поріг, комутатор тут же відреагує певними діями: блокування трафіку - повністю зупиняє підозрілий тип трафіку; запуск скрипту або команди CLI; обмеження швидкості передачі підозрілого типу трафіку; використання механізму «пасток» SNMP для відправки повідомлення на консоль мережевого управління.

Орієнтована на реалізацію інтегрованого підходу до управління трафіком і заснована на трьох ключових кроків - моніторинг, аналіз, реагування - технологія CLEAR-Flow гарантує масштабоване рішення складних проблем в швидкісних мережах і забезпечує гнучку модель, яка може адаптуватися до унікальних завдань конкретної мережі.

Включення в стратегію захисту даної технології якісним чином підвищить рівень інформаційної безпеки віртуальних інфраструктур хмар.

Список використаних джерел

1. *Ладигіна О.А. Перспективи захисту інформації в хмарних обчисленнях від атак на засоби віртуалізації / О.А. Ладигіна // Інформаційні технології та комп'ютерна інженерія: Науково-практична конференція, 4 груд. 2014: Збірн. тез. – Кіровоград: КНТУ, 2014. – С.164.*
2. *Ладигіна О.А. Дослідження загроз для віртуальної інфраструктури хмари та методи її захисту / О.А. Ладигіна // Інформаційна безпека держави, суспільства та особистості: Всеукраїнська науково-практична конференція, 16 квіт. 2015 року: Збірн. тез. – Кіровоград: КНТУ, 2015. – С.45-47.*
3. *Технология CLEAR-Flow: [Електронний ресурс] - Режим доступу: http://shop.nag.ru/uploads/Описание технологии управления сетевым трафиком CLEAR-Flow (rus).pdf.*