УДК 004

ОСОБЛИВОСТІ ВИБОРУ МІЖМЕРЕЖЕВИХ ЕКРАНІВ ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

Ільге І.Г., Ільге О.І., Запорожцев С.Ю.,

Харківський національний автомобільно-дорожній університет, Харків

Харківський національній університет радіоелектроніки, Харків

фірма «QUANLIFE», Львів

Захист комп'ютерних мереж від зовнішніх загроз є актуальною проблемою в сучасних умовах нашої країни. Одним з найбільш доцільних шляхів вирішення цієї проблеми є застосування міжмережевих екранів, що виконують функцію фільтрації вхідного і локального трафіку.

Залежно від способу реалізації міжмережевих екранів, вони можуть бути програмними або програмно-апаратними.

До першого типу відносять програмні засоби (firewall), що інсталюється на комп'ютер і забезпечує захист мережі від зовнішніх загроз. Це рішення зазвичай застосовують для невеликих локальних мереж.

Якщо треба захистити мережу більшого розміру, то застосовують програмні комплекси, які встановлюються на окремий виділений комп'ютер з достатньо потужними характеристиками.

В організаціях, що мають розвинену мережу зазвичай застосовують апаратно-програмні комплекси (security appliance), які, як правило, працюють на основі операційних систем FreeBSD або Linux. Також існує можливість застосування окремого модуля в штатному мережевому обладнанні - комутаторі, маршрутизаторі тощо.

При використанні апаратно-програмних комплексів можна отримати низку переваг, а саме підвищену швидкість обробки трафіку, більш просте управління захисними засобами, висока надійність захисту.

За технологією фільтрації трафіку розрізняють наступні види міжмережевих екранів:

- проксі-сервер;
- міжмережевий екран з контролем стану сеансів;
- міжмережевий екран UTM;
- міжмережевий екран нового покоління (NGFW);
- NGFW з активним захистом від загроз.

Проксі-сервер дозволяє створити міжмережевий екран на рівні додатку. Головним плюсом технології є забезпечення проксі повної інформації про додатки. Також вони підтримують часткову інформацію про поточне з'єднання. Але дана технологія має низку суттєвих обмежень, зокрема проксі не дозволяє забезпечувати proxy для протоколу UDP, обмежена можливість масштабування, недостатня продуктивність фільтрації і чутливість проксі-серверів до збоїв в операційних системах і додатках.

Принцип роботи міжмережевого екрану з контролем стану сеансів передбачає аналіз стану порту і протоколу, в результаті якого формується рішення про пропуск або блокуванні трафіку. При прийнятті рішення міжмережевий екран враховує не тільки правила, задані адміністратором, а й відомості, які були отримані з попередніх з'єднань.

Міжмережеві екрани типу UTM (Unified threat management) доцільно поєднують функції контент-фільтра, захисту від мережевих атак та антивірусного захисту, що підвищує ефективність і зручність управління мережевий захистом. Екран UTM може бути реалізований у вигляді програмного або програмно-апаратного комплексу. Програмні компоненти пристрою забезпечують створення багаторівневого мережевого доступу, підтримують фільтрацію URL, кластеризації, а також є функції антиспаму.

Екрани Next-Generation Firewall (NGFW) типу виконують всі основні функції, характерні для звичайних міжмережевих екранів. У тому числі вони забезпечують фільтрацію пакетів, підтримують VPN, здійснюють інспектування трафіку, перетворення портів і мережевих адрес. Вони здатні виконувати фільтрацію вже не просто на рівні протоколів і портів, а на рівні протоколів додатків і їх функцій.

Екрани типу NGFW повинні підтримувати такі ключові функції:

- захист мережі від постійних атак з боку систем, заражених шкідливим ПЗ;
- всі функції, характерні для першого покоління MME;
- розпізнавання типів додатків на основі IPS;
- функції інспекції трафіку, в тому числі додатків;
- настроюється точний контроль трафіку на рівні додатків;
- інспекція трафіку, шифрування якого виконується за допомогою SSL;
- підтримка бази описів додатків і загроз з постійними оновленнями.

NGFW з активним захистом від загроз ще більш підвищує надійність захисту мережі за рахунок підтримки можливостей звичайного NGFW та доповнення його функціоналу рядом нових можливостей, зокрема врахування контексту і виявлення на його основі ресурсів, що створюють підвищені ризики, автоматизацію функцій безпеки, що підвищує швидкодію і оперативність відображення мережевих атак, застосування кореляції подій на ПК і в мережі, що підвищує ефективність виявлення потенційно шкідливої активності, також значно полегшено адміністрування за рахунок впровадження уніфікованих політик.

При використанні міжмережевих екранів необхідно розуміти, що їх можливості по аналізу трафіку обмежені рамками ідентифікації та інтерпретації трафіку. Міжмережеві екрани не можуть також повністю взяти на себе функції антивірусного програмного забезпечення, тому їх потрібно використовувати в комплексі.

Таким чином, спираючись на конкретні вимоги організації є можливість вибрати міжмережевий екран одного з вище наведених типів з урахуванням наявних технічних та фінансових можливостей.

Література:

[1] Мережевий екран [Он-лайн]. Доступно: https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D0%B9_%D0%B5%D0%BA%D1%80%D0%B0%D0%BD.