infoDDoS

Безперервна робота ресурсів в мережі «Інтернет» завдяки комплексному захисту від DoS/DDoS-атак на базі платформи Radware DefensePro

infocom
TRUSTED SECURITY

Одним із найпоширеніших методів кібернападу є насичення інфраструктури клієнта великою кількістю зовнішніх запитів таким чином, що атаковане устаткування не може відповісти справжнім користувачам або відповідає настільки повільно, що стає фактично недоступним.

Як правило відмова атакованого сервісу досягається шляхом:

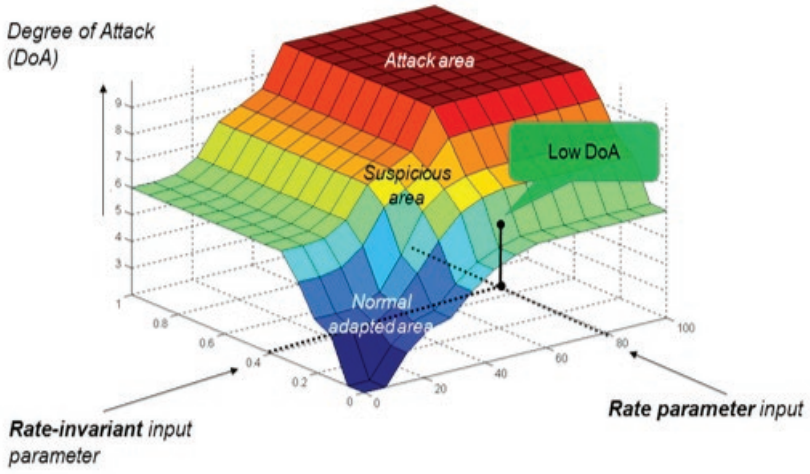
- примусу до повної зупинки роботи програмного забезпечення/устаткування атакованого сервісу, або до витрат наявних апаратних ресурсів, внаслідок чого устаткування не може продовжувати роботу;
- заняття комунікаційних каналів між користувачами і атакованим сервісом, вна слідок чого якість передачі даних перестає відповідати будь-яким (навіть самим мінімальним) вимогам.

Завдяки комплексу захисту infoDDoS на базі спеціалізованої платформи Radware DefensePro, ми можемо протистояти всім відомим типам DoS/DDoS атак та забезпечимо безперервну роботу Ваших ресурсів в інтернеті за допомогою багаторівневого захисту, який включає:

- поведінковий захист
- систему запобігання вторгнень
- захист від SYN-флуду
- обмеження одночасних з'єднань
- обмеження трафіку
- технологію SPI
- захист від сканування
- протидію http-атакам

- **Поведінковий захист (Behavioral DDoS Protection).**

Поведінковий захист - це найдієвіший і ресурсомісткий механізм захисту від DDoS-атак. В основі поведінкового захисту - глибока інспекція пакетів аж до 7-го рівня (Deep Packet Inspection), накопичення і аналіз статистики, навчання і адаптивна побудова багатовимірної моделі розподілу трафіку для штатних умов роботи мереж і мережевих сервісів, виявлення DDoS-атак на основі відхилень і аномалій, блокування нелегітимного трафіку методом динамічної фільтрації мережевих пакетів, з автоматичною генерацією поведінкових профілей (сигнатур) DDoS-атаки в реальному часі (модуль Fuzzy Logic).



Механізм поведінкового захисту має велику кількість точних налаштувань, підтримує періоди навчання тривалістю день, тиждень і місяць, дозволяє створювати окремі політики як для кожної мережі, що захищається, так і для кожного мережевого сервісу.

При виявленні ознак DDoS-атаки - час на прийняття рішення, побудову динамічних фільтрів і генерацію відповідних сигнатур становить всього **18** секунд.

В процесі придушення DDoS-атаки механізм поведінкового захисту відстежує кількісні та якісні параметри трафіку і при зниженні мережевої активності нижче критичних порогів знімає динамічні фільтри і деактивує сигнатури. Якщо застосування побудованих динамічних фільтрів і генерованих сигнатур не привело до зниження нелегітимного трафіку нижче порогових значень, то платформа Radware DefensePro здійснює аналіз додаткових параметрів трафіку з подальшим посиленням фільтрації та подальшою перегенерацією сигнатур.

Одна з найважливих переваг механізму поведінкового захисту платформи DefensePro – дієва протидія атакам впродовж першої хвилини (так званої «нульової хвилини»), для яких попередньо не створено статичних сигнатур (на підставі вже відомих атак) і не може бути застосований метод сигнатурного захисту.

• Система запобігання вторгнень (Intrusion Prevention System, IPS).

Платформа Redware DefensePro оснащена вбудованою системою запобігання зовнішніх вторгнень, яка є оптимальним рішенням протидії DDoS-атакам та високопродуктивним методом захисту від відомих вразливостей ПЗ. Крім цього, вона дозволяє виключити ризики проникнення «комп'ютерних черв'яків» та з легкістю виявляє роботу «ботів» на комп'ютерах співробітників.

Запорукою високої ефективності системи запобігання вторгнень є апаратна підтримка статичних сигнатур, які автоматично оновлюються компанією Radware в режими реального часу.

• Захист від SYN-флуду (TCP SYN Flood Protection).

Платформа Radware DefensePro має дуже ефективний механізм захисту від атак типу SYN-флуд з або без підміни IP-адреси відправника (spoofing). В основі - механізм SYN Cookies, котрий зберігає можливість отримання запитів на з'єднанная від справжніх клієнтів, незважаючи на поточну атаку.

• Обмеження одночасних з'єднань (Connection Limit)

Даний механізм захисту сервісу здійснює контроль максимально допустимої кількості сесій з IP-адреси відправника в одиницю часу і при перевищенні порогових значень блокує трафік з надмірно активних "хостів".

• Обмеження трафіку (BandWidth Management).

Даний механізм дозволяє виділити мінімально гарантовану смугу пропускання для заданого протоколу, що захищається, або мережевого сервісу та, при необхідності, обмежити смугу максимально допустимим значенням. Платформа DefensePro містить гнучкі механізми онлайнового моніторингу трафіку, оперативного інформування про інциденти, побудови розгорнутих звітів.

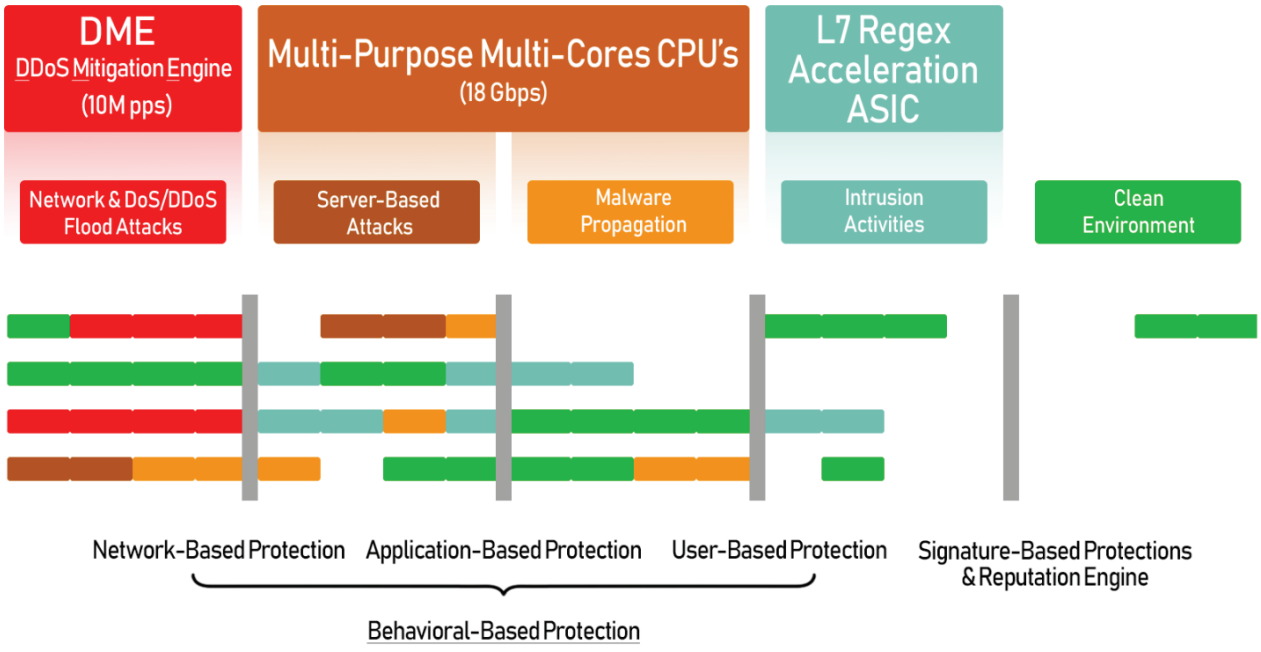
• **Технологія SPI (Stateful Packet Inspection)**

Даний механізм перевіряє протоколи TCP, ICMP, DNS, HTTPS, SMTP, IMAP, POP3, FTP і SSH на повну відповідність технічним специфікаціям та стандартам RFC. Механізм блокує атаки, засновані на порушенні послідовностей пакетів зазначених протоколів.

Апаратна платформа infoDDoS

Сервіс infoDDoS побудовано на базі спеціалізованої платформи Radware DefensePro з двома процесорами Dual-Core Opteron, з 10 Гбайт оперативної пам'яті, вбудованими високопродуктивними процесорами компанії EZChip Technologies, зі спеціалізованими ASIC і FPGA для апаратного прискорення обробки мережевого трафіку. DefensePro містить також високопродуктивний контекстний процесор NETL7 від компанії NetLogic Microsystems для апаратного прискорення сигнатурного аналізу мережевих пакетів.

Обробка мережевого трафіку здійснюється поетапно з використанням різних механізмів захисту.



Специфікація апаратної платформи:

- Max Legit Concurrent Sessions - 12,000,000
- Max Attack Concurrent Sessions - Unlimited
- Max DDoS Flood Attack Prevention Rate - 25,000,000 pps
- SSL/TLS Connections per Second - 95KCPS (RSA 2K)
- Latency < 60 micro seconds
- Real-Time Signatures - Detect attacks and protect in less than 18 seconds