Защита от киберугроз

Киберугрозы

Вредоносная программа (malware)—программное обеспечение, предназначенное для получения несанкционированного доступа к устройству.

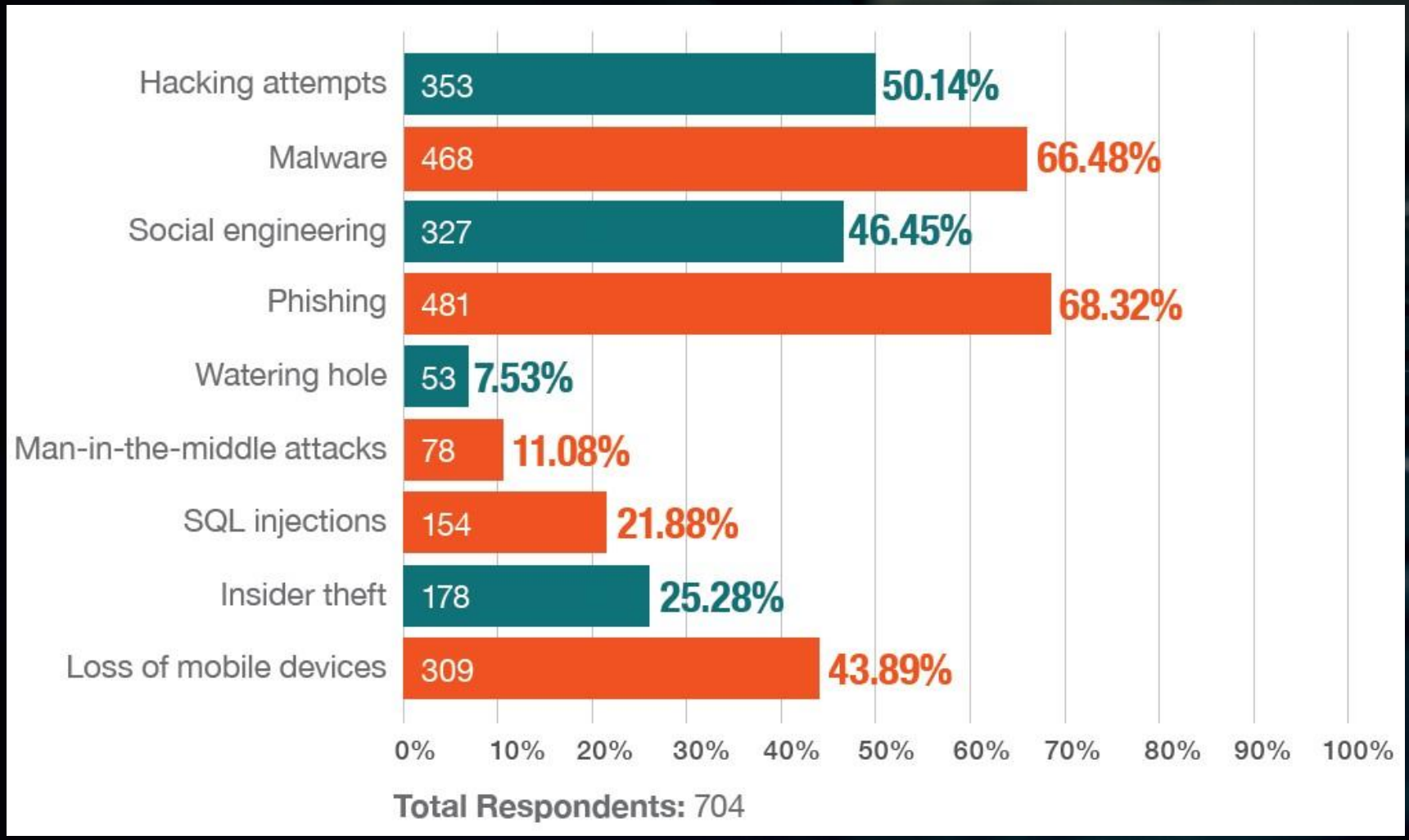
По методу размножения malware можно разделить на:

- **Эксплойт (exploit)** — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему (Shellshock, Heartbleed).
- **Троян** — вредоносная программа, не имеющая возможности распространяются самопроизвольно. Трояны распространяться исключительно людьми.
- **Компьютерный вирус** — вид вредоносного программного обеспечения, способного
создавать копии самого себя и внедряться в код других программ.
- **Сетевой червь** — разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети (Stuxnet).

0day (zero day) — термин, обозначающий неустранённые уязвимости, а также вредоносные программы, против которых ещё не разработаны защитные механизмы.

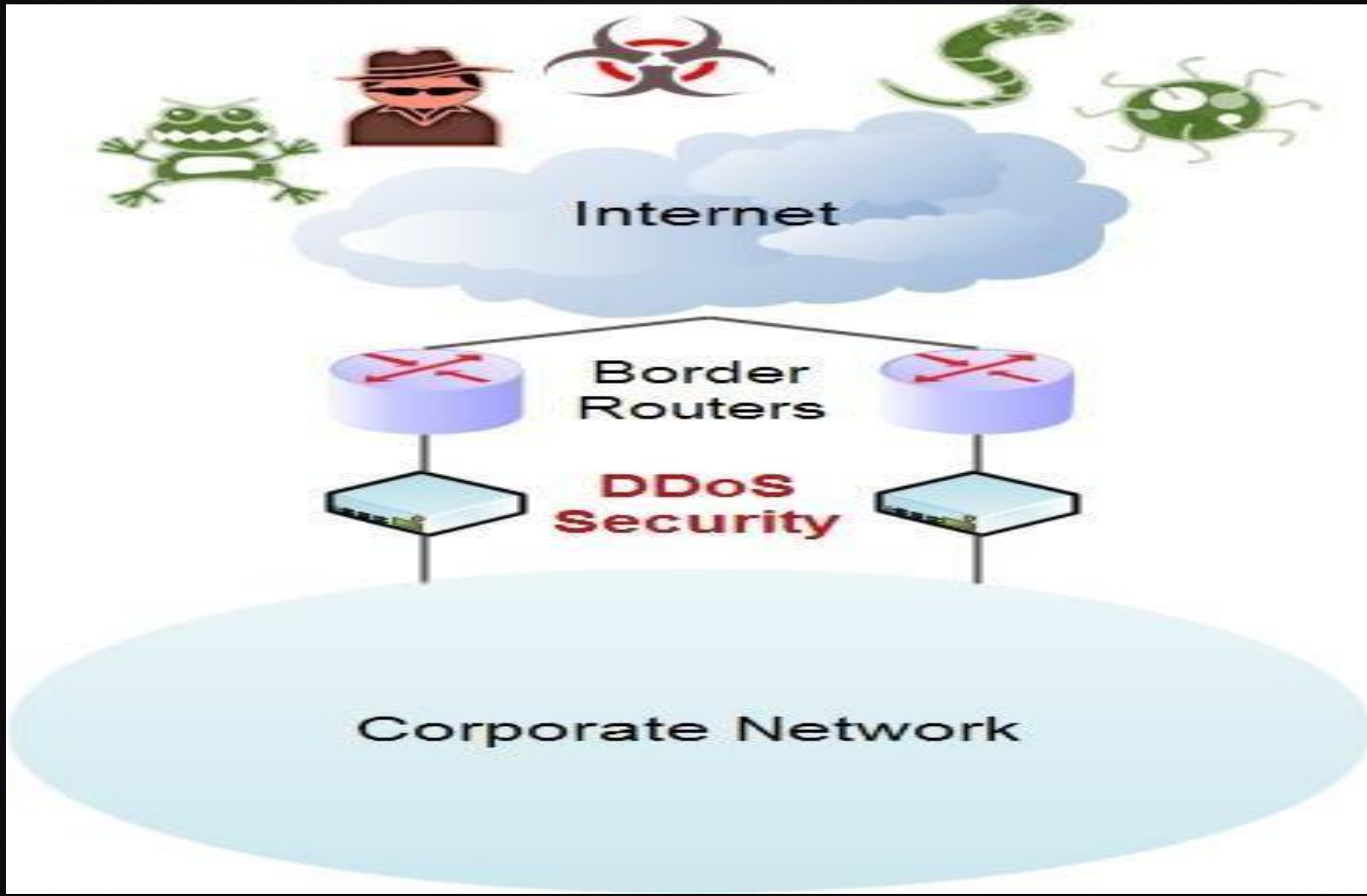
APT (Advanced Persistent Threat) – целенаправленные атаки на организацию, бизнес и т.д.

Рейтинг угроз



Согласно отчету ISACA - «Information System Audit and Control Association» (Ассоциация по аудиту и контролю информационных систем).

Первая линия обороны - защита от DDoS



Защита от DDoS

DoS (Denial of Service) — атака на вычислительную систему с целью довести её до отказа. Векторы DDoS атак:

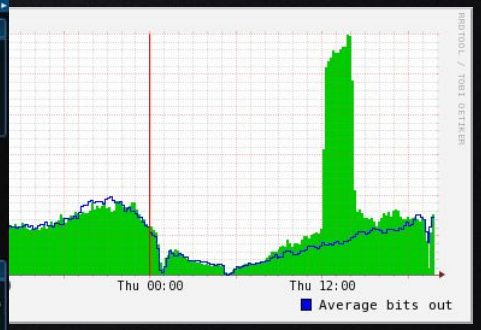
- **Volumetric** - объёмные атаки (UDP, ICMP, SYN флуд, DNS Amplification);
- **Low-And-Slow** - медленные, но опасные атаки (HTTP POST/GET flood, Slowloris).

Как правило для DDoS используют IP spoofing (подмену адреса отправителя) пакеты. Иногда DDoS это только прикрытие.

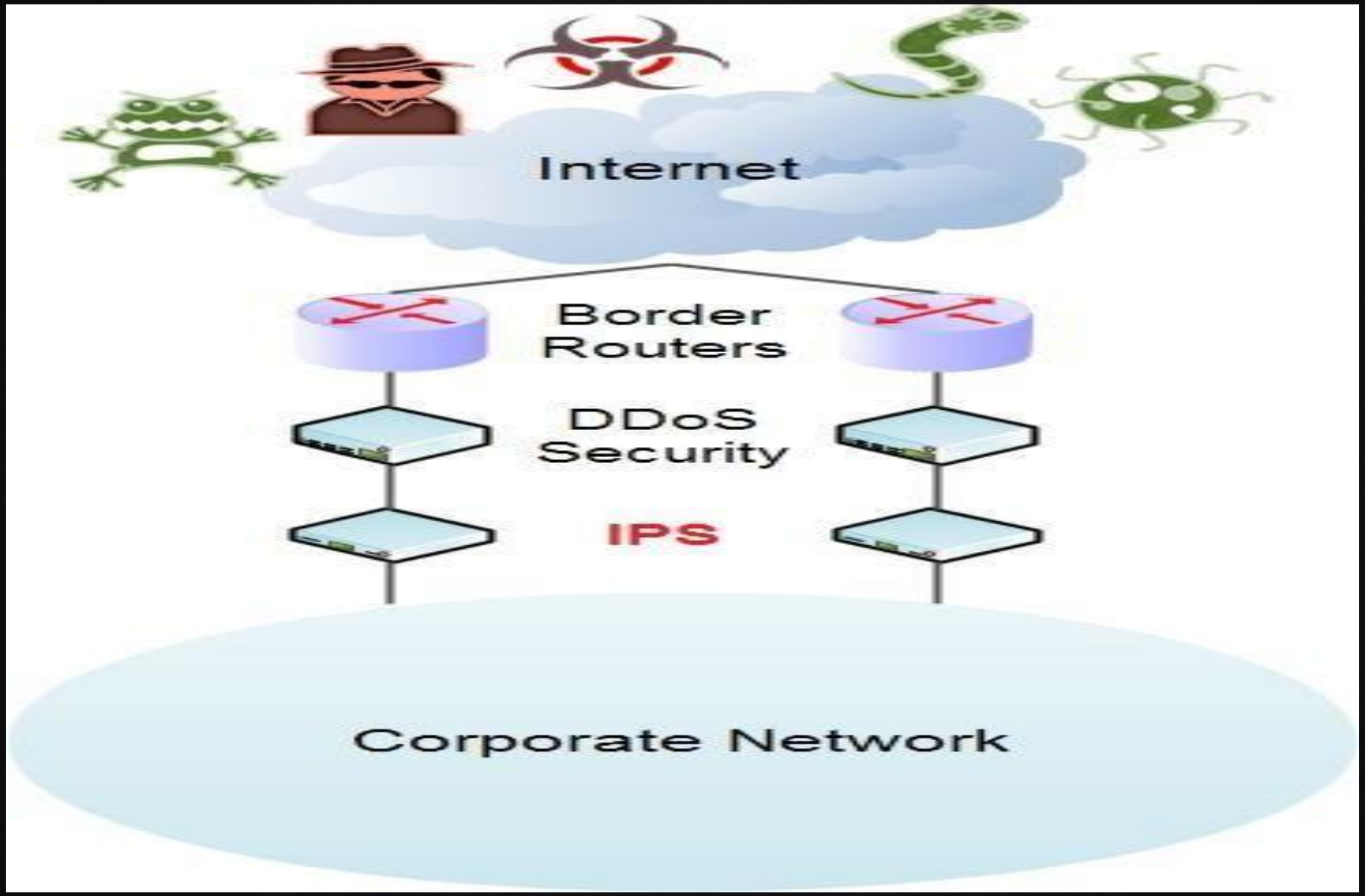
Борьба с DDoS атакой — это отбрасывание нелегитимных пакетов и пропуск легитимного трафика, между которыми проходит очень тонкая грань.

Обычные средства ACL либо Black Hole траффика устраивают далеко не всех.

Выход – использовать специализированные решения (комплексы).



Вторая линия обороны – предотвращение вторжений IPS



Использование IPS систем

Система предотвращения вторжений (Intrusion Prevention System) — система сетевой и компьютерной безопасности, **обнаруживающая вторжения** или нарушения безопасности и автоматически **защищающая от них**.

За счет использование технологии DPI (Deep Packet Inspection) данные устройства анализируют трафик 7-го уровня модели OSI.

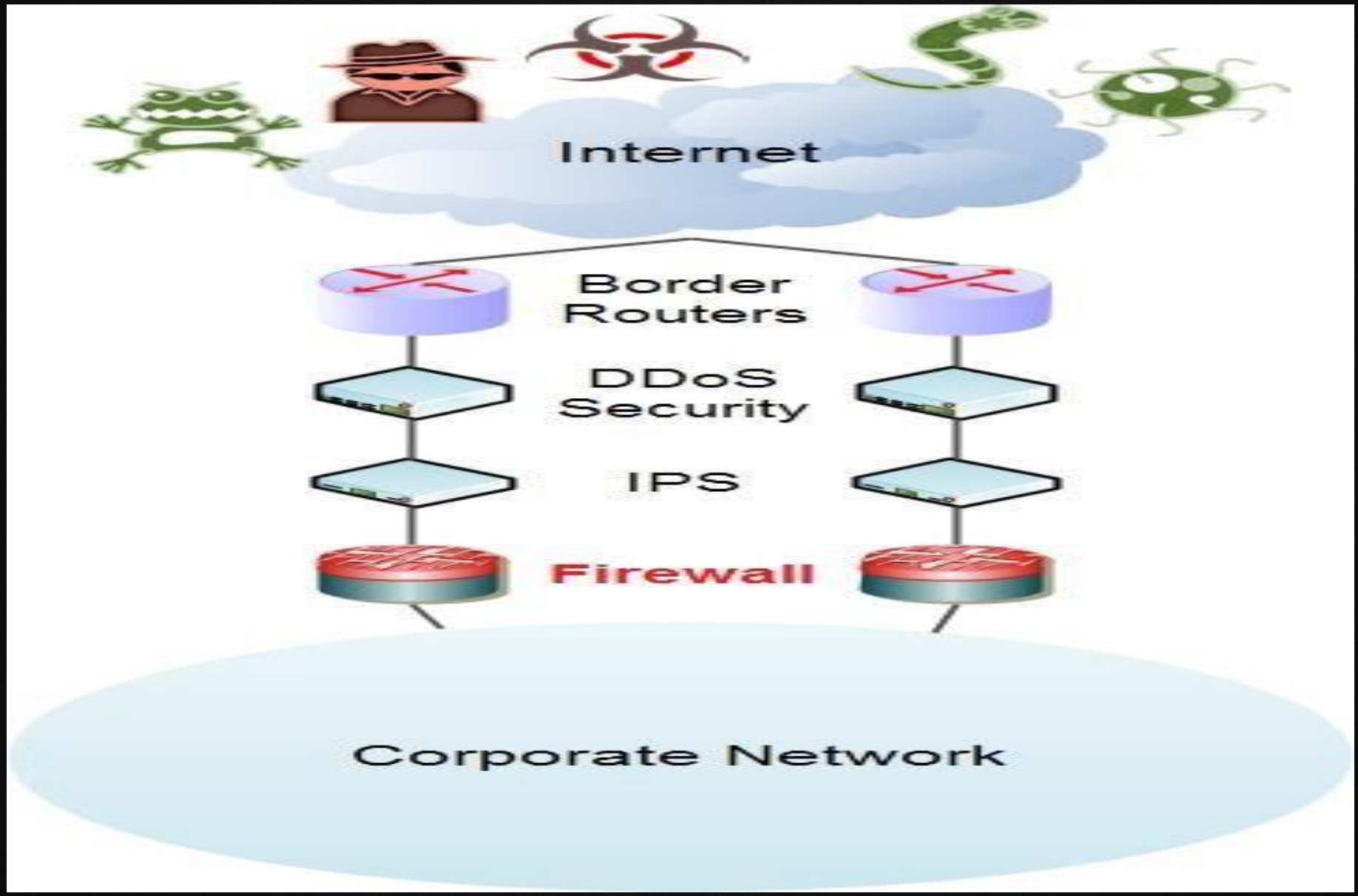
Системы IPS устанавливаться Inline, системы IDS (Intrusion Detection System) подключаются в режиме TAP и получают копию трафика без возможности влиять на нее.

Методы детектирования угроз:

- Signature-Based Detection (проверка трафика на основании существующих pattern-он);
- Statistical anomaly-based detection (сравнения штатного трафика с аномальным);
- Stateful [illegible] кола).

Список ведущих вендоров согласно лаборатории NSSLabs.

Третья линия обороны – Firewall



Использования Firewall

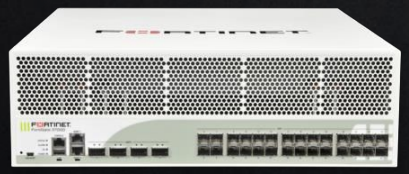
Межсетевой экран (Firewall) — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задача - защита компьютерных сетей или отдельных узлов от несанкционированного доступа методом определения политик.

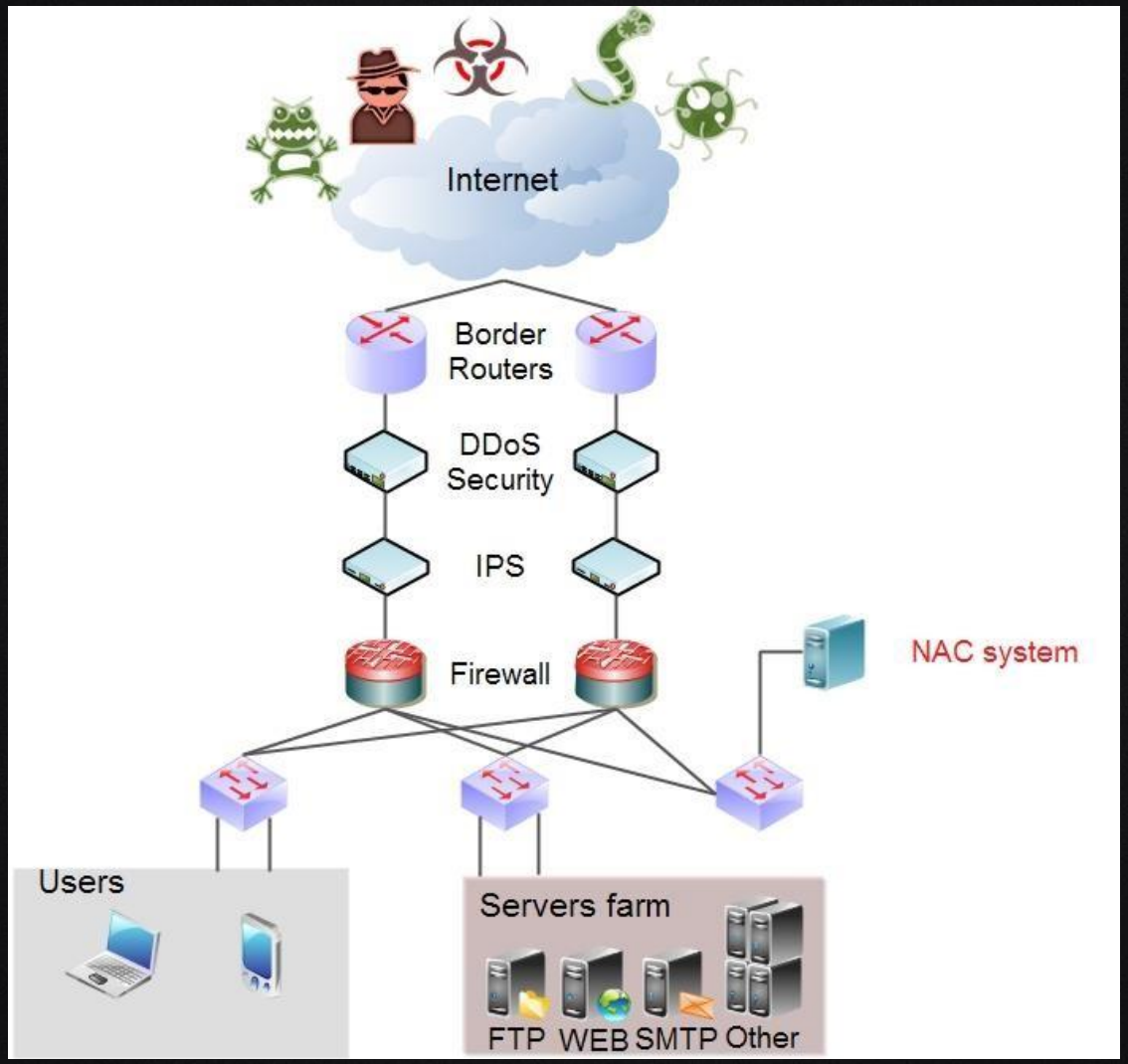
Основными функциями является: **Packet Filtering, NAT, VPN, Stateful Packet Inspection**.

Сейчас, зачастую, используют **Next Generation Firewall** к которому в отличии от обычного

Firewall добавлены следующие функции: IPS, Application Security, SSL Inspection, UTM (Antivirus, Antispam, Content filtering).

Оборона доступа – NAC



Использование **NAC** решений

NAC (Network Access Control) — комплекс технических средств и мер, обеспечивающий контроль доступа к сети на основании информации о пользователе и состоянии компьютера, получающего доступ в сеть, в частности на основе информации о его программном обеспечении.

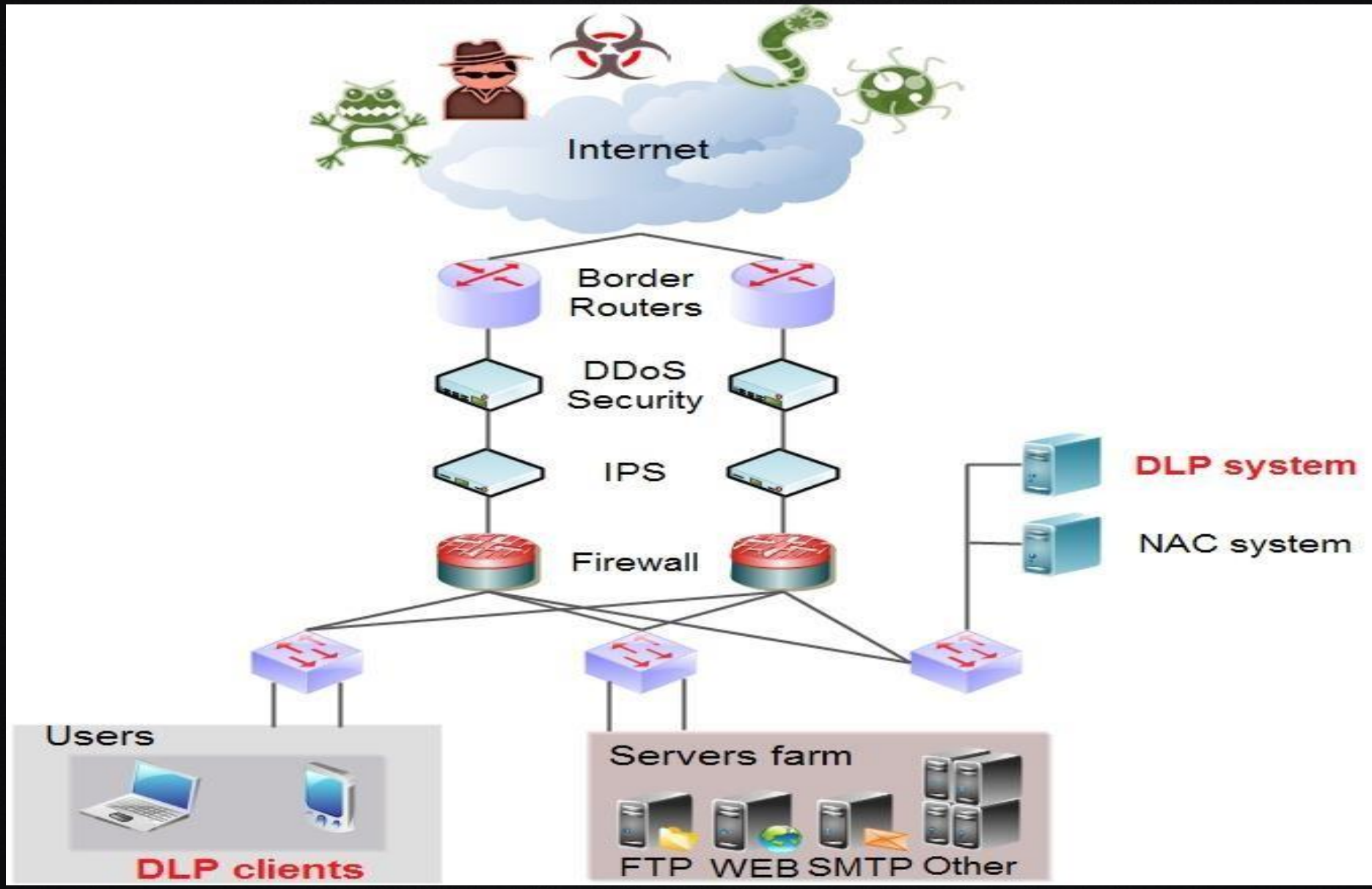
NAC обеспечивает контроль за тем, к каким участкам сети и к каким приложениям получит
доступ пользователь на основании:

- информации о пользователе, который подключается;
- информации о состоянии компьютера (установленное программное обеспечение, наличие обновлений и др.);
- времени подключения;
- точки подключения.

Правила контроля доступа могут применяться с помощью:

- Назначения пользователя в VLAN (802.1x);
- Применения ACL;
- Ограничений пропускной способности.

Защита от утечки изнутри- DLP



Использования DLP

Предотвращение утечек (Data Leak Prevention, DLP) — технологии предотвращения утечек конфиденциальной информации из информационной системы вовне.

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы.

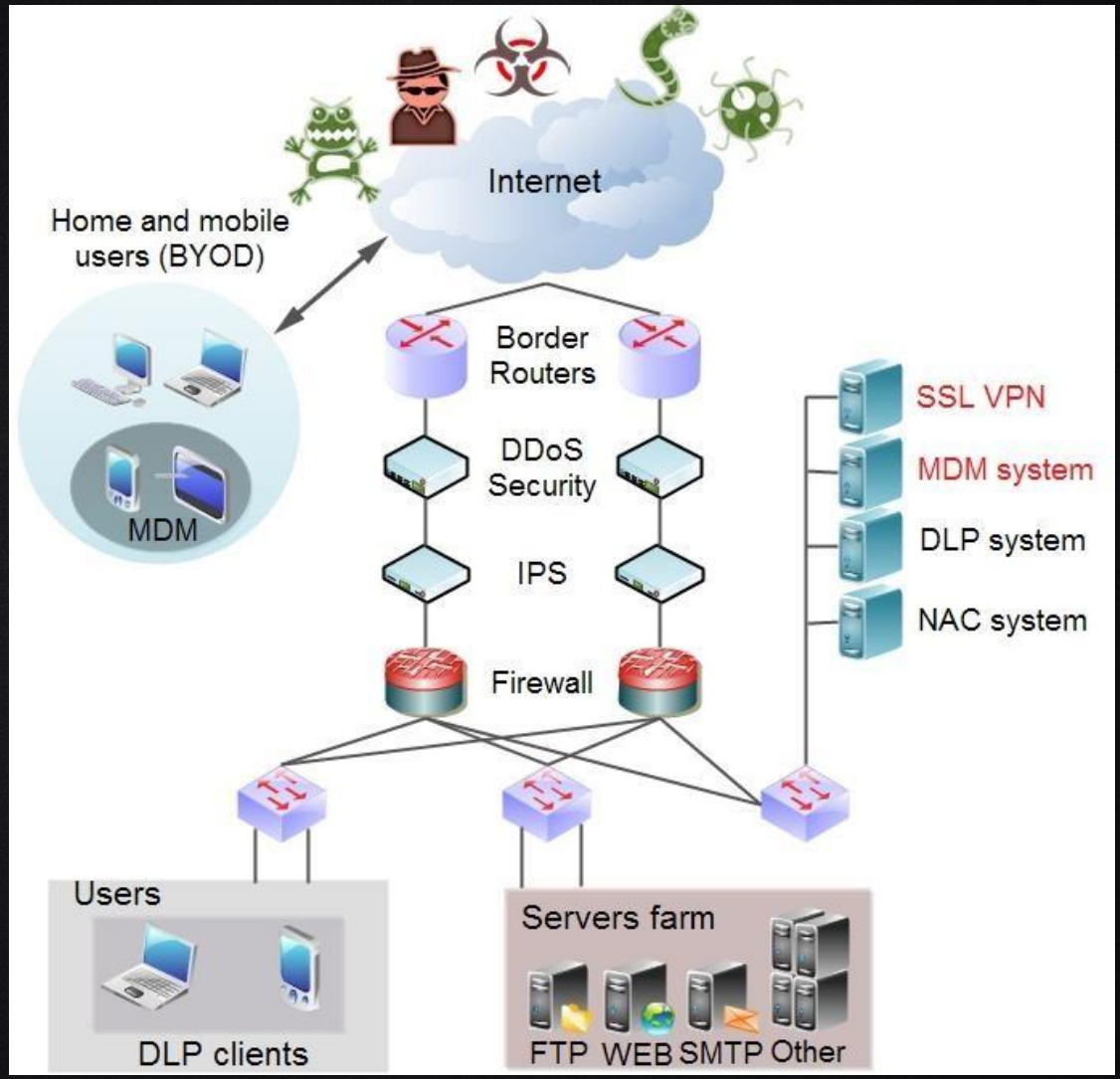
Основные функции DLP-систем

- контроль передачи информации через Интернет с использованием E-Mail, HTTP, HTTPS, FTP, Skype, ICQ и других приложений и протоколов;
- контроль сохранения информации на внешние носители - CD, DVD, flash, мобильные телефоны и т.п.;
- защита информации от утечки путем контроля вывода данных на печать;
- блокирование попыток пересылки/сохранения конфиденциальных данных, информирование администраторов ИБ об инцидентах, создание теневых копий, использование карантинной папки;
- поиск конфиденциальной информации на рабочих станциях и файловых серверах по ключевым словам, меткам документов, атрибутам файлов и цифровым отпечаткам.

Защита мобильных пользователей

Все болея популярным становиться работа на мобильных устройствах либо работа дома.

Такой подход к труду называется **BYOD (Bring Your Own Device)**.



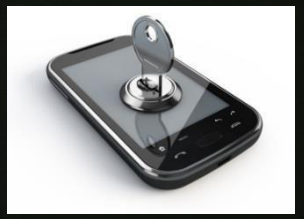
MDM - управление мобильными устройствами

Управление мобильными устройствами (Mobile device management, MDM) — набор сервисов и технологий, обеспечивающих контроль и защиту мобильных устройств (планшет, телефон), используемых организацией и её сотрудниками.

Корпоративные данные пользователя обрабатываться в отдельном «контейнере» (области) на устройстве.

Приемущества:

- Раздельное хранение корпоративных и личных приложений и данных
- Защита приложений и данных в контейнерах
- Предотвращение доступа бывших сотрудников к приложениям и данным
- Безопасный браузер
- Бэкап, перепрошивка
- Блокировка утерянного устройства.



Шифрованное подключения по SSL VPN

SSL VPN - Организация удалённого доступа **Virtual Private Network** посредством использования **Secure Sockets Layer** криптографического протокола.

Преимущества SSL VPN перед другими технологиями (IPSec):

- Достаточно одного лишь браузера чтоб получить доступ к ресурсу по защищённому каналу;
- Платформо-независимый доступ;
- Не имеет значения находитесь ли вы за NAT-ом, либо у вас закрыты все порты.

Фильтрация WEB и почтового трафика

Web Application Firewall (WAF) – имеет расширенные возможности анализа и фильтрации WEB-трафика. Использует сигнатуры, эвристику, двусторонний контроль трафика.

Защищает от: cross-site scripting, SQL injection, buffer overflows, file inclusion, denial of service, cookie poisoning, schema poisoning.

WEB и почтовая фильтрации способны в онлайн режиме производить сканирования запрашиваемых ресурсов и полученных писем на предмет вложенных угроз, спама.

С помощью глобальных (облачных) служб сбора информации, данные системы могут выполнять репутационную фильтрация.

Также, с помощью **WEB фильтрации на NGFW** можно гибко управлять доступом пользователей к ресурсам Интернет, выполнять фильтрацию по категориям (социальные сети, новости, поиск работы и тд.).

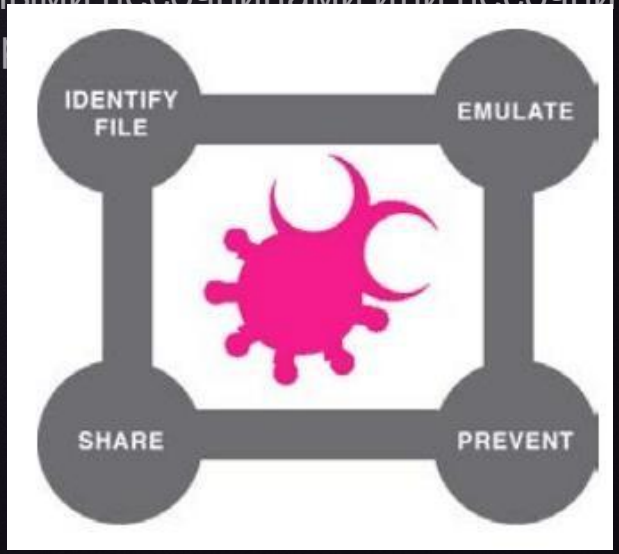
Обнаружение, основанное на эмуляции

Обнаружение, основанное на эмуляции — метод для обнаружения еще неизвестных вредоносных программ путем моделирования их поведения в песочнице.

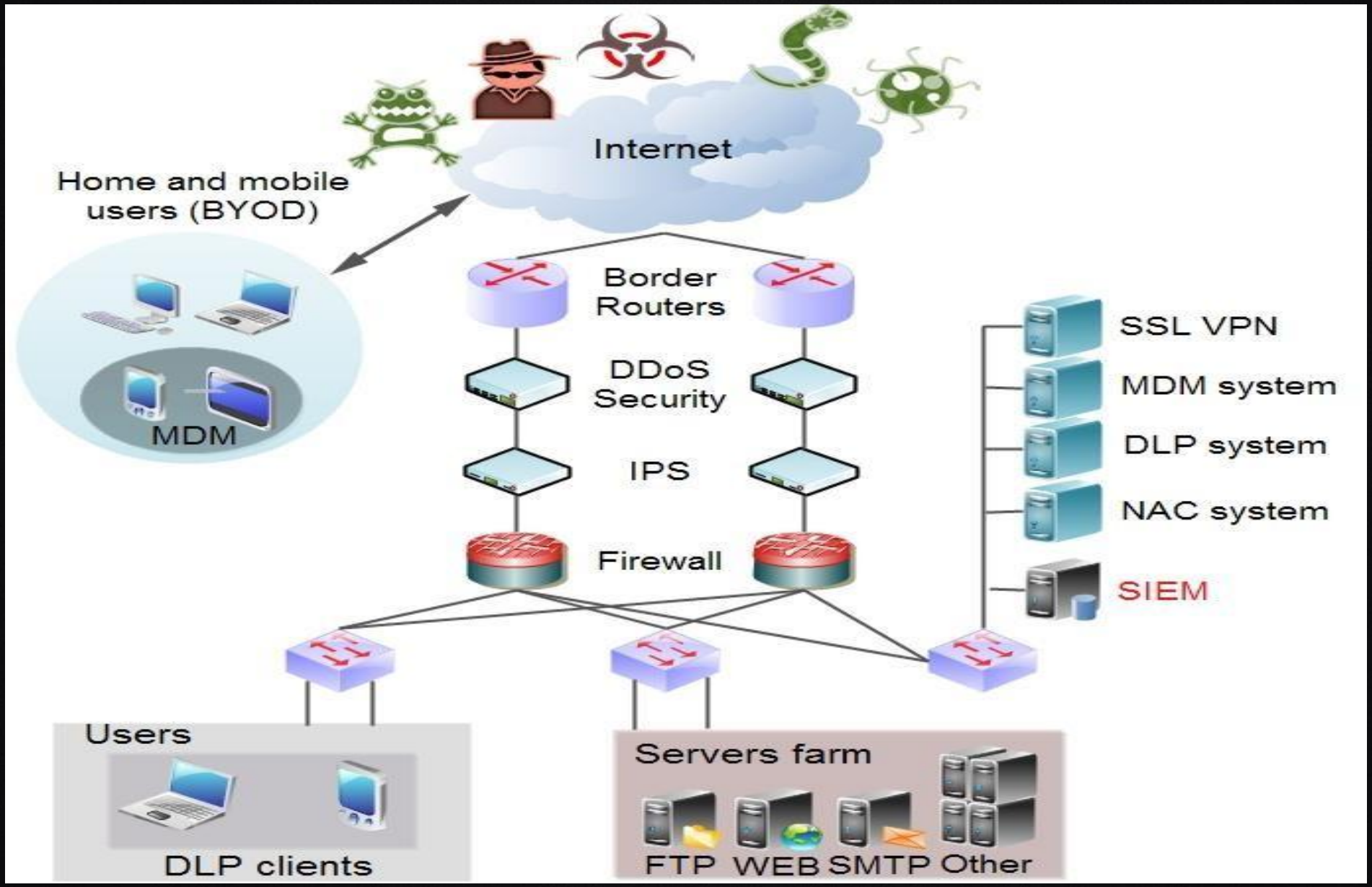
Песочница (sandbox) — специально выделенная среда (зачастую виртуальная) для безопасного исполнения компьютерных программ.

Как правило, песочницы используют для запуска непроверенного кода из неизвестных источников, как средство проактивной защиты от вредоносного кода, а также для обнаружения и анализа вредоносных программ.

Большинство NGFW обладают встроенными песочницами или песочницами в облаке. Также, существуют отдельные



Анализ всего происходящего - SIEM



Использования SIEM

SIEM (Security information and event management) – объединение двух терминов, обозначающих область применения ПО: SIM - Security information management - управление информационной безопасностью и SEM - Security event management - управление событиями безопасности.

Технология SIEM обеспечивает анализ в реальном времени событий (тревог) безопасности,
исходящих от сетевых устройств и приложений.

Функции: **Агрегация данных, Корреляция, Оповещение, Средства отображения, Хра**