Безопасность сети

Функции и типы фаерволов

**Фаервол (межсетевой экран, брандмауэр)** — это устройство или программное решение, которое контролирует сетевой трафик между разными сегментами сети и блокирует его при подозрении на вторжение или угрозу заражения. Мониторинг трафика важен для обеспечения безопасности, выявления проблем, защиты данных и оптимизации ресурсов сети.

К функциям фаерволов можно отнести:

* ***Контроль доступа***. Разрешение или блокировка трафика по IP-адресам, портам, протоколам;
* ***Разделение сетей***. Помогает изолировать внутренние сегменты, например, бухгалтерию от зоны разработчиков;
* ***Фильтрация содержимого***. Продвинутые фаерволы анализируют пакеты (Deep Packet Inspection), блокируя вредоносные или подозрительные данные;
* ***Защита от вторжений***. Современные решения могут интегрировать функции предотвращения атак.

## Типы фаерволов

**Аппаратные фаерволы** — это физические устройства, которые устанавливаются на границе сети (например, между локальной сетью и интернетом). Они обрабатывают трафик на аппаратном уровне, что обеспечивает высокую производительность даже при больших нагрузках.

Некоторые особенности аппаратных фаерволов:

* Работают в режиме inline, то есть напрямую в потоке сетевого трафика.
* Часто оснащены расширенными механизмами защиты, например, сигнатурным анализом или алгоритмами машинного обучения для выявления вредоносной активности.

**Программные фаерволы** – фаерволы, которые устанавливаются как приложения на операционную систему — сервер, рабочую станцию или маршрутизатор. Они контролируют трафик на уровне конкретного устройства, задают гибкие правила фильтрации.

Некоторые преимущества программных фаерволов:

* Гибкость настройки под конкретные задачи.
* Возможность интегрироваться с другими средствами киберзащиты, например, с системами класса EDR (Endpoint Detection and Response).

**Next-Gen фаерволы (NGFW)** — это усовершенствованные решения, которые фильтруют трафик не только на уровне протоколов и портов, но и на уровне приложений и их функций.

Некоторые особенности NGFW:

* Проактивно выявляют и блокируют вредоносный контент, который могут пропустить традиционные фаерволы.
* Контролируют приложения для предотвращения несанкционированного доступа к сети, блокируют вредоносные приложения.
* Фильтруют веб-трафик, чтобы предотвратить загрузку вредного контента.
* Используют данные об угрозах для выявления известных и неизвестных угроз.

### Инструменты мониторинга трафика:

Для мониторинга трафика можно использовать различные инструменты, среди них:

* ***Анализаторы протоколов***. Например, Wireshark (поддерживает более 2000 протоколов), tcpdump (консольный инструмент для захвата и анализа пакетов).
* ***Системы мониторинга сети***. К ним относятся Zabbix, PRTG Network Monitor, SolarWinds NPM.
* ***Инструменты активного тестирования***. Они генерируют тестовый трафик для измерения различных параметров сети. К ним относятся iPerf, PathPing, SmokePing.
* ***Инструменты предиктивной аналитики***. Эти решения используют машинное обучение для прогнозирования проблем производительности. К ним относятся Cisco AI Network Analytics, Splunk IT Service Intelligence, Elastic Machine Learning.

# Настройка правил фильтрации трафика

## Настройка правил фильтрации трафика (входящего/исходящего) в брандмауэре Windows 10:

* Запустить расширенный интерфейс межсетевого экрана.
* В окне брандмауэра кликнуть на «Дополнительные параметры».
* В левой навигационной панели выбрать «Правила для исходящего подключения». Система отобразит все созданные ранее правила.
* В правой панели кликнуть на «Создать правило». По умолчанию предлагается создать правило для программы, подтвердить выбор, нажав кнопку «Далее».
* Указать путь к исполняемому файлу программы для блокировки. Можно внести полный путь к exe-файлу вручную или воспользоваться кнопкой «Обзор».
* Определить, для каких сетей будет работать правило. Если нужно, чтобы правило применялось и в разных сетях, выбрать все опции. Если правило должно действовать только в одной из сетей, указать соответствующую опцию.
* Подтвердить выбор, нажав кнопку «Далее».
* Назвать правило. Можно указать описание правила, чтобы вспомнить причину его создания в дальнейшем.
* Завершить мастер, нажав кнопку «Готово».

### Настройка правил фильтрации трафика в Linux-файрволе с помощью iptables:

* Создать правило для входящих соединений. Указать цепочку INPUT, использовать ключ -i (—in-interface), чтобы определить входящий интерфейс, на который приходит ip-пакет. Завершить команду ключом -j (—jump), определяющим действие, которое будет выполнено для всех ip-пакетов, соответствующих критерию.
* Создать правило для уже установленных соединений. Использовать ключ -m, для загрузки модуля state, который даёт возможность определить текущее состояние ip-пакета.
* Установить политику по умолчанию, запрещающую все входящие соединения, не соответствующие правилам. Для этого в команде iptables служит ключ -P, устанавливающий политику по умолчанию для заданной цепочки.

# Виртуальная частная сеть (VPN)

**VPN (Virtual Private Network)** — это технология, которая позволяет передавать данные через открытую сеть общего пользования так, будто используется частная защищённая локальная сеть.

## Принципы работы VPN:

Шифрование — способ преобразования данных из читаемого формата в закодированный, который может быть расшифрован только специальным ключом. VPN-шифрование кодирует пользовательские данные, чтобы никто не мог их прочитать, в частности провайдеры и хакеры.

Туннелирование — сетевая технология, с помощью которой один тип протокола интегрируется в программу другого протокола. VPN-туннель — это зашифрованное соединение между устройством пользователя и сетью Интернет, которое обеспечивается VPN-сервисом.

## Типы VPN:

* ***Site-to-site VPN:***

Используется для создания защищённого туннеля между площадками. Например, между сетью главного офиса и сетью на удалённой площадке или в облаке.

**Преимущества:** позволяет организациям расширять свои сетевые ресурсы до филиалов, домашних офисов и сайтов бизнес-партнёров. Организации используют этот тип VPN, когда из-за расстояния нецелесообразно устанавливать прямые сетевые соединения между этими сайтами.

**Недостатки:** для установки и поддержания соединений site-to-site VPN требуется специальное оборудование.

* ***Remote Access VPN:***

Используется для подключения отдельных пользователей к частным сетям организаций с помощью VPN-клиента.

**Преимущества:** позволяет подключать практически любые приложения для работы с данными, голосом или видео на удалённом устройстве. С помощью современных технологий VPN можно проводить проверки безопасности на конечных точках перед подключением к сети.

**Недостатки:** из-за неправильной настройки запросы могут отправляться в незашифрованном виде в обход VPN, и злоумышленник может получить информацию об IP-адресе устройств или сети, посещённых веб-сайтах и их IP-адресах.

* ***SSL VPN:***

Работает через интернет, обычно через веб-браузер, а не через установку приложения на клиентском компьютере. SSL VPN даёт пользователям удалённый доступ к конкретной системе или приложению в сети.

**Преимущества**: функция SSL VPN уже встроена в современные веб-браузеры, что позволяет пользователям из любого места с доступом в интернет устанавливать соединения VPN. Технология SSL VPN может помочь повысить производительность сотрудников и снизить затраты на программное обеспечение и поддержку VPN-клиента.

**Недостатки:** помогает только для защиты трафика от веб-браузера до веб-сервера.

* ***IPSec VPN:***

Работает на сетевом уровне и обеспечивает полное шифрование всего трафика. IPSec VPN защищает любой трафик между двумя точками, определёнными по IP-адресам.

**Преимущества:** один из самых надёжных способов безопасной передачи трафика. Протокол широко поддерживается и интегрирован во многие устройства.

**Недостатки:** IPSec VPN требователен к вычислительным ресурсам и сложен для реализации, из-за чего могут возникать проблемы с совместимостью оборудования VPN. При большом числе мобильных пользователей обслуживание IPSec VPN (включая обновление и настройку конфигурации клиентского ПО) обходится слишком дорого.

**Intrusion Detection System**

**IDS (Intrusion Detection System)** — система обнаружения вторжений. Это программное или аппаратное средство, которое предназначено для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими.

## Принцип работы

IDS анализирует сетевой трафик и поведение пользователей с помощью различных методов:

* Сигнатурный анализ. Поиск известных шаблонов атак, основанный на базе данных с сигнатурами угроз.
* Анализ на основе аномалий. Выявление подозрительных отклонений от нормы в сетевом поведении.
* Гибридный метод. Сочетает сигнатурный и поведенческий анализ для повышения точности обнаружения атак.

## Функции IDS

* Мониторинг сетевого трафика и анализ действий пользователей и приложений в реальном времени.
* Выявление аномалий (отклонений) от нормального поведения в сети или на хостах.
* Сигнатурный анализ. Использование предопределённых шаблонов (сигнатур) для обнаружения известных атак.
* Уведомления и оповещения. Отправка уведомлений администраторам при обнаружении потенциальных угроз.
* Журналирование событий. Ведение подробных логов всех выявленных аномалий и инцидентов.

# Intrusion Prevention System

**IPS (Intrusion Prevention System)** — система предотвращения вторжений. Это программное или аппаратное решение, которое обнаруживает несанкционированные действия и атаки, а также автоматически противодействует им.

## Принцип работы

IPS анализирует сетевой трафик в режиме реального времени, выявляет подозрительную активность и немедленно предпринимает меры для её предотвращения. Например, если система определяет, что в сеть пытается проникнуть вредоносное ПО или происходит распределённая атака типа DDoS, она немедленно прерывает такие попытки и блокирует подозрительные пакеты.

## Функции IPS

* Обнаружение потенциально опасной активности. IPS сравнивает трафик с известными сигнатурами атаки, выявляет отклонения от нормы или нарушения политик безопасности.
* Противодействие вредоносной активности. Система блокирует IP-адрес, с которого поступает вредоносный трафик, отсеивает входящие пакеты с потенциально опасными данными, разрывает соединение.
* Интеграция с другими системами безопасности. IPS работает в связке с фаерволами и антивирусными программами для комплексной защиты.